Rec'd PCT/PTO 04 APR 2005
530238

特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年1 月27 日 (27.01.2005)

PCT

(10) 国際公開番号
WO 2005/008954 A1

(51) 国際特許分類[7]: H04L 9/08, G06F 13/00

(21) 国際出願番号: PCT/JP2004/008942

(22) 国際出願日: 2004 年6 月18 日 (18.06.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-175085 2003 年6 月19 日 (19.06.2003) JP
特願2003-176568 2003 年6 月20 日 (20.06.2003) JP
特願2003-176569 2003 年6 月20 日 (20.06.2003) JP

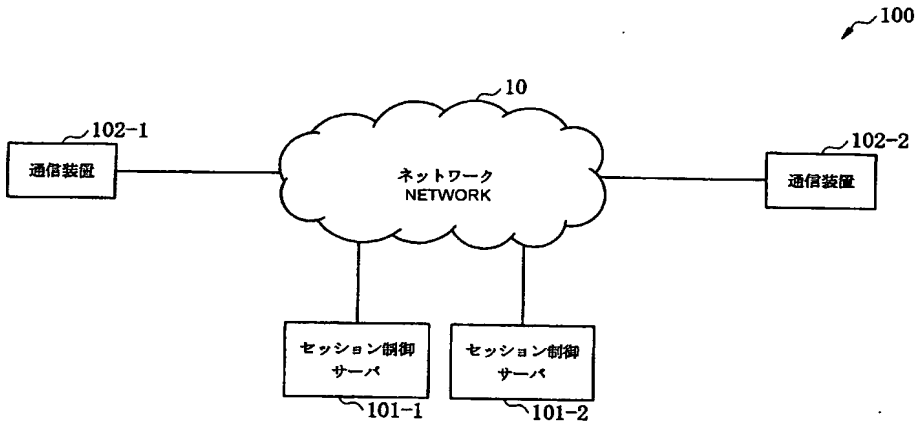
(71) 出願人 (米国を除く全ての指定国について): 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒100-8116 東京都千代田区 大手町二丁目３番１号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 小野 久美子 (ONO,Kumiko) [JP/JP]; 〒180-8585 東京都 武蔵野市 緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 立元 慎也 (TACHIMOTO,Shinya) [JP/JP]; 〒180-8585 東京都 武蔵野市 緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP). 坂谷 精一 (SAKAYA,Seiichi) [JP/JP]; 〒180-8585 東京都 武蔵野市 緑町３丁目９－１１ ＮＴＴ知的財産センタ内 Tokyo (JP).

[続葉有]

(54) Title: SESSION CONTROL SERVER AND COMMUNICATION SYSTEM

(54) 発明の名称: セッション制御サーバ及び通信システム



102-1...COMMUNICATION DEVICE
102-2...COMMUNICATION DEVICE
101-1...SESSION CONTROL SERVER
101-2...SESSION CONTROL SERVER

(57) Abstract: A communication device is communicably connected to a session control server via a network and establishes a session with another communication device by transmitting/receiving a signal to/from the session control server. The communication device includes: means for creating a non-symmetric key pair; request means for requesting the session control server to issue a certificate for the public key of the non-symmetric key pair; reception means for receiving notification of public key certificate issuance completion from the session control server; storage means for storing the public key certificate received; transmission means for transmitting a request for registering the position of the communication device to the session control server; and reception means for receiving notification of the position registration completion including a valid term from the session control server. The position registration request and the certificate issuance request are transmitted together as a single request.

(57) 要約: ネットワークを介してセッション制御サーバと通信可能に接続され、セッション制御サーバとの間で信号送受信を行うことによって他の通信装置とのセッションを確立する通信装置は、非対称鍵ペアを作成する手段と、セッション制御サーバに対して非対称鍵ペアのうち

[続葉有]

WO 2005/008954 A1

BEST AVAILABLE COPY

(74) 代理人: 志賀 正武 (SHIGA,Masatake); 〒104-8453 東京都 中央区 八重洲２丁目３番１号 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書
— 補正書・説明書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

の公開鍵に対する証明書発行を要求する要求手段と、セッション制御サーバから公開鍵証明書発行完了の通知を受信する受信手段と、受信した公開鍵証明書を記憶する記憶手段と、セッション制御サーバに対して通信装置の位置の登録要求を送信する送信手段と、セッション制御サーバから有効期間を含む位置登録完了の通知を受信する受信手段とを備え、位置登録要求と証明書発行要求とを一括した要求を送信する。

明 細 書

セッション制御サーバ及び通信システム

技術分野

本発明は、セッション制御サーバに関する。本発明は、より詳細には、本発明は、電子証明書発行およびその管理を行うセッション制御サーバと、その電子証明書を利用して通信を行う通信装置と、通信システムと、その通信方法、ならびにその通信方法を実行させるためのプログラムとそれを記録した記録媒体に関する。また、本発明は、信号の中継を行うセッション制御サーバ、暗号鍵に基づいて暗号化された通信を行う通信装置および通信システム、その通信方法、ならびにそのプログラムとそれを記録した記録媒体に関する。さらに、本発明は、信号の中継を行うセッション制御サーバ、暗号鍵に基づいて暗号化された通信を行う通信装置、通信システムおよび通信方法、ならびにそれらを用いたプログラムとそれを記録した記録媒体に関する。

本願は、２００３年６月１９日に出願された特願２００３－１７５０８５号、ならびに２００３年６月２０日に出願された特願２００３－１７６５６８号および特願２００３－１７６５６９号に対し優先権を主張し、その内容をここに援用する。

背景技術

従来から用いられている電子証明書の発行サーバ、電子証明書の管理サーバや認証局としては、ＬＤＡＰ（Ｌｉｇｈｔｗａｉｇｔ Ｄｉｒｅｃｔｏｒｙ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ）サーバや、Ｗｅｂ（Ｗｏｒｌｄ Ｗｉｄｅ Ｗｅｂ）サーバが挙げられる。前者は、Ｘ．５００ベースのディレクトリ管理データベースにアクセスするためのプロトコルであって、ディレクトリサーバ上のディレクトリ情報の作成、変更、削除、検索などの操作が可能である。後者は、インターネット上にハイパーテキストを構築し、あらゆる情報をアクセス可能にする

ことを目的としており、クライアントとサーバとの通信プロトコルにはＨＴＴＰが用いられる。

これらのサーバの利用方法では、電子証明書の利用者が、暗号化通信を行う場合に、必要に応じて通信相手の電子証明書を取得する必要がある。

また取得した電子証明書について、認証局リンクをたどったり、ＣＲＬ（失効リスト）を取得するなどして、有効性を判断する必要もある。

上記に関しては、インターネットの標準化機関であるＩＥＴＦ（Ｉｎｔｅｒｎｅｔ　Ｅｎｇｉｎｅｅｒｉｎｇ　Ｔａｓｋ　Ｆｏｒｃｅ）がとりまとめている規格書の中で、ＲＦＣ（Ｒｅｑｕｅｓｔ　ｆｏｒ　Ｃｏｍｍｅｎｔｓ）２５１１（Ｉｎｔｅｒｎｅｔ　Ｘ．５０９　Ｃｅｒｔｉｆｉｃａｔｅ　Ｒｅｑｕｅｓｔ　Ｍｅｓｓａｇｅ　Ｆｏｒｍａｔ）がある。

通信相手が複数の電子証明書を所持し、有効期間も様々である場合、電子証明書の利用者は、セッションを開始する際に、どの電子証明書を利用するのが適当であるかを判断するために、電子証明書の管理サーバから、通信相手に対応する複数の電子証明書を取得して、各々について有効性を判断する必要があった。

また、有効であると判断した証明書を利用して、信号を送信しても、受信元の通信装置において、その証明書を利用可能な状態に設定していない場合には、受信側で復号化できず、セッション開始処理が遅延するという問題があった。

さらに、通信相手のデジタル署名に含まれる電子証明書を受信した場合に、受信した証明書が有効か否かを判断するため、ＬＤＡＰサーバに接続する処理などを行う場合には、セッションの開始処理が遅延するという問題もあった。

また、従来から用いられているユーザ間の通信情報の暗号化方式としては、ＩＰＳｅｃ（Ｓｅｃｕｒｉｔｙ　ａｒｃｈｉｔｅｃｔｕｒｅ　ｆｏｒ　Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）、ＴＬＳ（Ｔｒａｎｓｐｏｒｔ　Ｌａｙｅｒ　Ｓｅｃｕｒｉｔｙ）、Ｓ／ＭＩＭＥなどが挙げられる。

中継サーバが、情報を参照できる暗号化方式としては、ＩＰＳｅｃ、ＴＬＳがある。

ＩＰＳｅｃは、ＴＣＰ／ＩＰの通信のセキュリティを強化するための技術であって、データをＩＰカプセル化してトンネリングする手法を規定するＥＳＰ（Ｅ

ｎｃａｐｓｕｌａｔｉｏｎ Ｓｅｃｕｒｅ Ｐａｙｌｏａｄ）、ユーザ認証用のデータをＩＰデータに組み込むＡＨ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｈｅａｄｅｒ）などがある。ＴＬＳは、バンキングシステムなど、クライアント・サーバ間のセキュリティが必要なアプリケーションで広く用いられる。

ＩＰＳｅｃ、ＴＬＳの方法では、転送区間の始点、終点間で、暗号化鍵や方式の調整を行い、その結果に基づく暗号化通信を行い、通信装置が送受する伝達情報の機密性を向上させている。

しかし、ＩＰＳｅｃやＴＬＳなどの暗号化方式では、転送区間の始点、終点間で暗号化方式、鍵の調整を行い、暗号化／復号化の処理を転送区間の始点および終点で行う必要があった。そのため、信号中継を行うセッション制御サーバで、情報の復号化を必ず行うことになり、セッション制御サーバに対する情報保護が可能な暗号化通信が困難であった。

Ｓ／ＭＩＭＥは、エンド・エンド間のセキュリティのためのものであり、エンド・エンドで暗号化した際、中継サーバでは、情報を参照できない。具体的には、Ｓ／ＭＩＭＥの暗号化方式では、発着通信装置間で暗号化を行い、全てのセッション制御サーバに対して情報保護が可能であるが、特定のセッション制御サーバに情報開示が必要な場合であっても、情報開示が不可能であるという問題があった。

上記に関しては、インターネットの標準化機関であるＩＥＴＦ（Ｉｎｔｅｒｎｅｔ Ｅｎｇｉｎｅｅｒｉｎｇ Ｔａｓｋ Ｆｏｒｃｅ）がとりまとめている規格書の中で、ＲＦＣ（Ｒｅｑｕｅｓｔ ｆｏｒ Ｃｏｍｍｅｎｔｓ）３２６１Ｓｅｃｔｉｏｎ２６．２がある。

発明の開示

本発明の第１の目的は、上記のような従来の課題を解決し、セッション通信を行う通信装置に対して有効な電子証明書を配布でき、ユーザへのセッション確立時の有効性確認を容易にすることが可能な電子証明書管理機能を具備するセッション制御サーバ、およびそのサーバを用いて通信を行う通信装置、通信システム

および通信方法、ならびにそのプログラムとそのプログラムを記録する記録媒体を提供することにある。

本発明は、次のような機能を有する。

（1）あるユーザAが、自分の通信装置A'の位置登録要求を行うに当って、非対称鍵ペアを作成し、その鍵ペアの中の公開鍵に対する証明書発行要求と、位置登録要求とを一括してセッション制御サーバに送信する（請求項1参照）。

（2）セッション制御サーバが、通信装置A'から上記（1）の要求を受信し、ユーザ認証した上で証明書を発行し、位置情報の有効時間とともに記憶する（請求項5参照）。

（3）上記（1）の処理を行った通信装置A'は、上記（2）の処理を行ったセッション制御サーバからの位置登録完了通知と証明書発行完了通知とを、有効時間とともに受信し、これを記憶する（請求項2参照）。

（4）あるユーザAが、自分の通信装置A'の位置登録要求を行うに当って、非対称鍵ペアとその鍵ペアの中の公開鍵に対する証明書を既に所有しているときは、位置登録要求と証明書登録要求とを一括してセッション制御サーバに送信する（請求項3参照）。

（5）セッション制御サーバが、通信装置A'から上記（2）の要求を受信し、証明書の有効性を判断して、ユーザ認証を行った上で、証明書の登録を有効時間のある位置登録とともに記憶する（請求項5参照）。

（6）上記（4）の処理を行った通信装置A'は、上記（5）の処理を行ったセッション制御サーバからの位置登録完了通知と、証明書発行完了通知とを有効時間とともに受信し、これを記憶する（請求項4参照）。

（7）通信装置B'がセッション開始に先立ち、通信相手Aの公開証明書をセッション制御サーバに対して問い合わせる。

（8）セッション制御サーバは、証明書問い合わせ要求を受信し、その問い合わせ対象の通信相手Aについて、通信装置A'の公開鍵証明書の有効性を確認し、これを通信装置B'に通知する（請求項6参照）。

本発明においては、位置情報の管理およびセッション制御を行うサーバが、電子証明書（公開鍵証明書）の管理を行うため、通信装置における実有効性を保証した配布が可能になる。

また、電子証明書の配布時には、位置情報の管理およびセッション制御を行うサーバによって電子証明書の有効性が確認されているため、セッション制御信号内で使用する電子証明書の有効性を、認証局などに問い合わせることなく確認することが可能になる。

本発明の第２の目的は、上記のような従来の課題を解決し、発着ユーザ間通信のエンド・エンド間の機密性を確保しながら、かつ、情報開示が必要な特定のセッション制御サーバに対してのみ情報開示を可能とするセッション制御サーバ、通信装置、通信システムおよび通信方法、ならびにそのプログラムと記録媒体を提供することにある。

本発明においては、

（９）通信装置Ａがセッション確立のための信号送信に先立ち、信号内の情報の暗号化のための第一の暗号化鍵（対称暗号鍵）を生成する。

通信装置Ａは、送信先の通信装置Ｂの第二の暗号化鍵（公開鍵あるいは事前共有鍵）と、通信装置Ａがセッション確立に伴い情報を開示する対象である０以上のセッション制御サーバの第二の暗号化鍵（公開鍵あるいは事前共有鍵）とを用いて、個々の第二の暗号化鍵毎に第一の暗号化鍵を暗号化する。

通信装置Ａは、第一の暗号化鍵で、情報を暗号化する。暗号化する前に、情報に対して署名を付与してもよい。

通信装置Ａは、第一の暗号化鍵で暗号化した情報とともに、各第二の暗号化鍵（個々の公開鍵あるいは事前共有鍵）で暗号化した第一の暗号化鍵と、復号化要求指示とをセッション制御サーバに送信する。

なお、ここでの復号化要求指示は、通信装置Ａがセッション確立に伴い情報を開示する対象であるセッション制御サーバを、セッション制御サーバを示す識別子の形で陽に提示していてもよいし、陽に提示していなくてもよい。

また、復号化対象のコンテンツＩＤについても、陽に提示していてもよいし、陽に提示していなくてもよい。

陽に提示していない場合には、例えばセッション確立に伴い経由される個々のセッション制御サーバが、自らの保持する第二の暗号化鍵に対応する第二の復号化鍵による第一の暗号化鍵の復号化を行い、得られた情報が第一の暗号化鍵を示す表現形式に合致していれば、自らが復号化要求を受けたセッション制御サーバであること判断できる。このため、第二の暗号化鍵で暗号化された第一の暗号化鍵自体が復号化要求指示となる（請求項１６参照）。

（１０）通信装置Ａもしくは他のセッション管理サーバからの信号を受信したセッション制御サーバは、復号化要求の有無と復号化対象の情報とを判断し、復号化要求があった場合、自らの第二の暗号化鍵に対応する第二の復号化鍵によって第一の暗号化鍵の復号化を行う。もしくは、自らの第二の暗号化鍵に対応する第二の復号化鍵により第一の暗号化鍵の復号化を行い、その結果から復号化要求の有無を判断する。または、これらのいずれをも行う。これらは、（９）に記載した通信装置における復号化要求によって決まる。

いずれの場合も、得られた第一の暗号化鍵を用いて、暗号化情報の復号化を行う（請求項１７参照）。

（１１）上記（１０）のセッション制御サーバは、更に、暗号化した第一の暗号化鍵を、セッション単位に記憶する。セッション制御サーバは、この第一の暗号化鍵をその後の当該セッションの情報の復号化の際に再利用する（請求項１８参照）。

（１２）通信装置Ｂは、暗号化された第一の暗号化鍵が添付された暗号化情報を含む信号を受信し、第一の暗号鍵の復号化を行い、その第一の暗号鍵を用いて、暗号化情報の復号化を行う。通信装置Ｂは、セッション単位に第一の暗号化鍵を記憶し、同一セッション内の情報の暗号化に前記第一の暗号化鍵を再利用する。

通信装置Ｂは、第一の暗号化鍵を暗号化した情報が添付されない暗号化情報を含む信号を送信する。同一セッション内の情報の復号化にも第一の暗号化鍵を再利用する（請求項１９参照）。

（１３）通信装置Ａは、セッション単位に第一の暗号化鍵を記憶し、第一の暗号化鍵を暗号化した情報が添付されない暗号化情報を含む信号を受信した際に、同

一セッション内の情報の復号化に、および、同一セッション内の　情報の暗号化に、前記第一の暗号化鍵を再利用する（請求項２０参照）。

（１４）通信装置Ａおよび通信装置Ｂは、セッション内で、一定時間経過後あるいは一定回数使用後、第一の暗号化鍵を更新し、更新信号とともに送信する（請求項２１，２２参照）。

（１５）セッション制御サーバは、セッション内で通信装置Ａ（あるいは通信装置Ｂ）から第一の暗号化鍵の更新信号を受信すると、記憶していたそのセッションの第一の暗号化鍵を更新し、更新信号とともに通信装置Ｂ（あるいは通信装置Ａ）に送信する（請求項２３参照）。

本発明においては、情報開示を行うセッション制御サーバを指定して、情報開示を行いながら安全な信号内の情報の送受信が可能となる。通信装置間の暗号化情報を含む信号通信の場合でも、特定のセッション制御サーバによる情報の参照が可能となるため、その情報を基に通信制御が可能となる。

本発明の第３の目的は、上記のような従来の課題を解決するため、信頼できる宛先との間のセキュリティ確保が可能となるようなセッション制御サーバ、通信装置、通信システムおよび通信方法、ならびにそのプログラムと記録媒体を提供することにある。

上記セキュリティ確保の区間としては、発ユーザと特定の信頼できるセッション制御サーバの間、特定の信頼できるセッション制御サーバと特定の信頼できるセッション制御サーバの間、および特定の信頼できるセッション制御サーバと着ユーザ間という転送区間に依存しない任意の区間である。

本発明においては、情報の暗号化のために、通信装置もしくはセッション制御サーバで生成される暗号化鍵を第一の暗号化鍵と呼び、第一の暗号化鍵を暗号化するための暗号化鍵を第二の暗号化鍵と呼ぶ。

（１６）通信装置Ａがセッション確立のための信号送信に先立ち、信号内の情報の暗号化のための第一の暗号化鍵（対称暗号鍵）を生成する。

通信装置Ａは、送信先の通信装置Ｂの第二の暗号化鍵（公開鍵あるいは事前共有鍵）、もしくは、通信装置Ａがセッション確立に伴って情報の開示のみ、もし

くは開示と変更の両方を許容するセッション制御サーバの第二の暗号化鍵（公開鍵あるいは事前共有鍵）のいずれかを用いて、第一の暗号化鍵を暗号化する。

通信装置Ａは、第一の暗号化鍵で、情報を暗号化する。暗号化する前に、情報に対して署名を付与してもよい。

通信装置Ａは、第一の暗号化鍵で暗号化した情報とともに、上記いずれかの第二の暗号化鍵（公開鍵あるいは事前共有鍵）で暗号化した第一の暗号化鍵と、第二の暗号化鍵がセッション制御サーバの暗号化鍵の場合は、さらに復号化要求指示をセッション制御サーバに送信する。

なお、ここでの復号化要求指示は、通信装置Ａがセッション確立に伴い情報の開示もしくは開示と変更を許諾する対象であるセッション制御サーバを、セッション制御サーバを示す識別子の形で陽に提示していてもよいし、陽に提示していなくてもよい。

陽に提示していない場合、例えば、セッション確立に伴い経由される個々のセッション制御サーバが、自らの保持する第二の暗号化鍵に対応する第二の復号化鍵による第一の暗号化鍵の復号化を行い、得られた情報が第一の暗号化鍵を示す表現形式に合致している場合に、自らが復号化要求を受けたセッション制御サーバであると判断できる。このため、第二の暗号化鍵で暗号化された第一の暗号化鍵自体が復号化要求指示となる。

また、ここでの情報の開示のみなのか、もしくは開示と変更の両方が許容されているか否かの違いは、例えば、対象となる情報に発信側通信端末による電子署名が付与されているか否か（例えば、付与されている場合は、開示のみが許容されている）などによって決定してもよい（請求項３７参照）。

（１７）通信装置Ａもしくは他のセッション制御サーバからの信号を受信したセッション制御サーバは、復号化要求の有無を判断し、復号化要求があった場合、自らの第二の暗号化鍵に対応する第二の復号化鍵により第一の暗号化鍵の復号化を行う。もしくは、自らの第二の暗号化鍵に対応する第二の復号化鍵により第一の暗号化鍵の復号化を行い、その結果から復号化要求有無を判断する。または、これらのいずれをも行う。これらは、（１６）および（１７）の後半に記載の通信装置およびセッション制御サーバにおける復号化要求によって決まる。

いずれの場合も、得られた第一の暗号化鍵を用いて、暗号化情報の復号化を行う。

次に、このセッション制御サーバは、復号化して得た第一の暗号化鍵を、次段のセッション制御サーバあるいは着ユーザの第二の暗号化鍵（公開鍵あるいは事前共有鍵）で暗号化する。そして、第一の暗号化鍵で暗号化された情報、および第二の暗号化鍵で暗号化された第一の暗号化鍵を、次段のセッション制御サーバあるいは着ユーザに送信する。なお、送信の際に、第二の暗号化鍵がセッション制御サーバの暗号化鍵の場合には、復号化要求指示もセッション制御サーバに送信する（請求項３８参照）。

（１８）なお、上記（１７）のセッション制御サーバにおいて、新たに第一の暗号化鍵（対称暗号鍵）を生成し、その鍵を使用して復号化された情報を暗号化してもよい。そして、その生成された第一の暗号化鍵を、次段のセッション制御サーバあるいは着ユーザの第二の暗号化鍵（公開鍵あるいは事前共有鍵）で暗号化する。それらをセッション制御サーバあるいは着ユーザに送信する。なお、送信の際に、第二の暗号化鍵がセッション制御サーバの暗号化鍵の場合には、復号化要求指示もセッション制御サーバに送信する（請求項３９参照）。

（１９）セッション制御サーバは、受信した第一の暗号化鍵、生成した第一の暗号化鍵を、セッションおよび対向装置単位に管理する。セッション制御サーバは、第一の暗号化鍵を、その後の情報の暗号化または復号化に再利用する（請求項４０参照）。

（２０）通信装置Ｂは、暗号化された第一の暗号化鍵が添付された暗号化情報を受信し、第一の暗号化鍵の復号化を行い、その第一の暗号化鍵を用いて、暗号化情報の復号化を行う。通信装置Ｂは、応答信号を送信する際に、復号化した第一の暗号化鍵を再利用して、情報を暗号化する。通信装置Ｂは、第一の暗号化鍵を添付せず、暗号化した情報を送信する。第一の暗号化鍵を記憶し、同一セッションでかつ同一対向装置の信号の暗号化および復号化に再利用する（請求項４１参照）。

（２１）通信装置Ａは、セッションと対向装置単位に第一の暗号化鍵を記憶し、第一の暗号化鍵を暗号化した情報が添付されない暗号化情報を含む信号を受信し

た際に、同一セッションでかつ同一対向装置の情報の復号化に利用する。また、同一セッションでかつ同一対向装置に信号を送信する際の情報の暗号化に、前記第一の暗号化鍵を再利用する（請求項４２参照）。

（２２）通信装置Ａ、および通信装置Ｂは、セッション内で一定時間経過後あるいは一定回数使用後に、第一の暗号化鍵を更新し、更新信号と共に送信する（請求項４３，４４参照）。

（２３）セッション制御サーバは、通信装置Ａ（あるいは通信装置Ｂ）から更新信号を受信すると、記憶していた第一の暗号化鍵を更新し、更新信号を通信装置Ｂ（あるいは通信装置Ａ）に送信する。その際に、新たに生成した第一の暗号化鍵を生成して、通信装置Ｂ（あるいは通信装置Ａ）に送信してもよい（請求項４５参照）。

本発明においては、情報開示を行うセッション制御サーバを指定して情報開示を行いつつ、安全な情報の送受信が可能となる。特定のセッション制御サーバによる情報の参照および／または変更が可能となるため、その情報をもとに通信制御が可能になる。

図面の簡単な説明

図１は、本発明の第１の実施形態に係る通信システムの構成図である。

図２は、図１における通信装置の詳細ブロック構成図である。

図３は、図１におけるセッション制御サーバの詳細ブロック構成図である。

図４は、本発明の第１の実施例に係る通信装置の送信信号例を示す図である。

図５は、本発明の第１の実施例に係る通信装置の受信信号例を示す図である。

図６は、本発明の第３の実施例に係るセッション制御サーバの受信信号例を示す図である。

図７は、本発明の第３の実施例に係るセッション制御サーバの送信信号例を示す図である。

図８は、本発明の第２の実施例に係るセッション制御サーバと通信装置の処理フローチャートである。

図９は、本発明の第３の実施例に係るセッション制御サーバと通信装置の処理フローチャートである。

図１０は、本発明の第２の実施形態に係る通信システムのブロック構成図である。

図１１は、図１０におけるセッション制御サーバの詳細な構成図である。

図１２は、図１０における通信装置の詳細な構成図である。

図１３は、本発明の第２の実施形態に係る通信装置（２０２－１）の送信信号例を示す図である。

図１４は、本発明の第２の実施形態に係る通信装置（２０２－２）の送信信号例を示す図である。

図１５は、本発明の第４の実施例に係る通信方法の説明図である。

図１６は、本発明の第５の実施例に係る通信方法の説明図である。

図１７は、本発明の第６の実施例に係る通信方法の説明図である。

図１８は、本発明の第３の実施形態に係る通信システムの構成図である。

図１９は、図１８におけるセッション制御サーバのブロック構成図である。

図２０は、図１８における通信装置のブロック構成図である。

図２１は、本発明の第３の実施形態に係る通信装置（３０２－１）の送信信号例の図である。

図２２は、本発明の第３の実施形態に係る通信装置（３０２－２）の送信信号例の図である。

図２３は、本発明の第７の実施例に係る通信方法の説明図である。

図２４は、本発明の第８の実施例に係る通信方法の説明図である。

図２５は、本発明の第９の実施例に係る通信方法の説明図である。

発明を実施するための最良の形態

以下、図面を参照しつつ、本発明の好適な実施例について説明する。ただし、本発明は以下の各実施例に限定されるものではなく、例えばこれら実施例の構成要素同士を適宜組み合わせてもよい。

以下、本発明の実施の形態を、図面を参照して詳細に説明する。

（第１の実施形態）

［システム構成］

図１は、本発明の第１の実施形態に係る通信システムの構成図である。

図１に示すように、通信システム１００は、ネットワーク１０を介して通信可能に接続された１台以上のセッション制御サーバ１０１と、複数の通信装置１０２を含むように構成されている。

また、通信装置１０２は、本発明による手順に従って、セッション制御サーバ１０１を介して暗号化通信により通信を行う。なお、通信システム１００においては、セッション制御サーバ１０１が２台用意されているが、２台に限定されるものではない。また、通信装置１０２が２台用意されているが、２台に限定されるものではない。

なお、本発明においては、通信装置１０２は、パソコン、携帯端末あるいはゲートウェイなどの通信機器を含み、ネットワーク１０の構成は、有線、無線を問わない。

以降は、説明の便宜を図るために、通信装置１０２－１を発信側とし、通信装置１０２－２を着信側として説明する。セッション制御サーバ１０１－１が通信装置１０２－１を収容しており、セッション制御サーバ１０１－２が通信装置１０２－２を収容しているものとして説明する。

セッション制御サーバ１０１－１，１０１－２は、それぞれ通信装置１０２－１と通信装置１０２－２から位置登録要求と公開鍵証明書の発行要求あるいは登録要求とを受信し、位置登録情報と公開鍵証明書とを記憶する。

［通信装置］

図２は、本発明の第１の実施形態に係る通信装置のブロック構成図である。

図２に示すように、通信装置１０２は、信号送信手段１１０、セッション制御手段１１１、位置登録要求手段１１２、位置登録通知受信手段１１３、非対称鍵生成（記憶）手段１１４、証明書発行（登録）要求手段１１５、位置情報および公開鍵証明書記憶手段１１６、信号受信手段１１７および証明書通知受信手段１１８を含むように構成される。

ここで、１１４は、非対称鍵記憶手段であるとともに、非対称鍵生成手段でもあり、また、１１５は証明書登録要求手段であるとともに、証明書発行要求手段でもある。従って、以後は、一方を括弧内にして併記する。なお、１１４，１１５は、これら一方だけの機能を備えたものであってもよい。

通信装置１０２－１は、非対称鍵記憶（生成）手段１１４によって生成（記憶）した公開鍵について、証明書登録（発行）要求手段１１５で要求信号によって作成し、位置登録要求手段１１２によって生成された位置登録要求信号と合わせて、セッション制御手段１１１に送る。

セッション制御手段１１１で生成した信号を、信号送信手段１１０よってセッション制御サーバ１０１に送信する。

その後、通信装置１０２－１は、セッション制御サーバ１０１－１から位置登録完了通知信号を受信し、セッション制御手段１１１によって信号内容を解析し、位置登録通知受信手段１１３に送る。

公開鍵証明書が添付されている場合は、証明書通知受信手段１１８によってこれを受信し、位置情報および公開鍵証明書記憶手段１１６に、位置情報と公開鍵証明書とをともに記憶する。

これにより、通信装置１０２－１が使用可能な公開鍵証明書を入手した状態となり、公開鍵を使用した暗号化情報を含む信号受信、および、公開鍵証明書を使用したデジタル署名を添付した信号送信が可能となる。このように信号送信時に、デジタル署名を添付することにより、発着のユーザ間の相互認証、サーバによるユーザ認証、およびユーザの信号送信の否認防止が可能となる。

（第１の実施例）

第１の実施例は、通信装置１０２－１がセッション制御サーバ１０１－１に対して位置登録および証明書発行を要求し、セッション制御サーバ１０１－１から位置登録と証明書発行の完了通知を受けるまでのやりとりである。なお、位置登録および証明書発行要求には、位置登録要求が含まれるが、証明書発行要求は含まれることもあれば含まれないこともある。

図４は、図２の通信装置における送信信号例を示す図、および、図５は、図２の通信装置における受信信号例を示す図である。

ここでの通信装置１０２－１の相手は、セッション制御サーバ１０１－１である。例えば、図４に示す通信装置１０２－１からの送信信号は、ＲＦＣ３２６１に準拠したＳＩＰメッセージの１つであるＲＥＧＩＳＴＥＲメソッド４００であり、そのメッセージに通信装置の位置情報が、要望する有効時間と共に設定されている（４０２）。また、公開鍵証明書要求およびユーザ認証キーも設定されている（４０２）。これらの情報は、機密性を保つために、コンテンツ暗号化鍵で暗号化され、Ｓ／ＭＩＭＥのＥｎｖｅｌｏｐｅｄ－Ｄａｔａ（４０１）として送信される。

コンテンツ暗号化鍵の暗号化のための鍵暗号化鍵としては、セッション制御サーバ１０１－１の公開鍵を用いてもよいし、セッション制御サーバ１０１－１と通信装置１０２－１の使用者との間の事前共有鍵（パスワードなど）を用いてもよい。

図５に示すように、セッション制御サーバ１０１－１が受信する信号は、ＲＥＧＩＳＴＥＲメソッドに対する正常応答２００　ＯＫ（５００）であって、そのメッセージに、登録された位置情報と、セッション制御サーバ１０１－１が認めた有効時間とが設定されている（５０４）。これらの情報は、機密性を保つために、暗号化鍵で暗号化され、ＥｎｖｅｌｏｐｅｄＤａｔａ内に設定されている（５０２）。また、公開鍵証明書も設定されている（５０４）。

信号の復号化では、まず暗号化されたコンテンツ暗号化鍵（５０５）の復号化を行う。

暗号化鍵の復号化には、通信装置１０２－１の秘密鍵を用いてもよいし、セッション制御サーバ１０１－１と通信装置１０２－１の使用者との間の事前共有鍵（パスワードなど）を用いてもよい。

復号化したコンテンツ暗号化鍵で、暗号化した情報（５０４）を復号化する。

受信した位置情報と公開鍵証明書とは、有効時間とともに、位置情報および公開鍵証明書記憶手段１１６に記憶される。

改竄有無の検出のために、サーバのデジタル署名（５０３）が添付されていれば、その署名を確認してもよい。

[セッション制御サーバ]

図３は、本発明の第１の実施形態に係るセッション制御サーバのブロック図である。

図３に示すように、セッション制御サーバ１０１は、信号受信手段１２０、セッション制御手段１２１、信号送信手段１２２、証明書発行（登録）要求受信手段１２３、証明書発行（有効性確認）手段１２４、位置登録要求受信手段１２５、位置情報および公開鍵証明書記憶手段１２６、公開鍵証明書問合せ要求受信手段１２７、および公開鍵証明書通知送信手段１２８を具備している。

ここで、１２３は、証明書発行要求受信手段と証明書登録要求受信手段との両方の機能を備えており、１２４は、証明書発行手段と証明書有効性確認手段との両方の機能を備えている。なお、１２３，１２４は、上記の２つの機能のうちの一方だけを備えていてもよい。

信号受信手段１２０は、通信装置１０２－１から位置登録要求信号を受信する。セッション制御手段１２１は、受信した位置登録要求信号が位置登録要求信号であると判断すると、この位置登録要求信号を位置登録要求受信手段１２５に送る。

位置登録要求手段１２５は、ユーザ認証正常終了後、証明書発行要求が添付されていると判断すると、証明書発行要求受信手段１２３に必要な情報を提供する。証明書発行要求受信手段１２３は、要求内容が正当であることを確認し、証明書発行手段１２４がユーザに対して証明書を発行する。

発行した証明書と位置情報とは、位置情報および公開証明書記憶手段１２６に記憶される。

セッション制御手段１２１は、位置情報および公開鍵証明書の情報を含めた応答信号を生成し、通信装置１０２－１に信号送信する。

（第２の実施例）

第２の実施例、セッション制御サーバ１０１－１が、通信装置１０２－１から位置登録および証明書発行の要求を受け、通信装置１０２－１に位置登録および証明書発行の完了通知を送信するまでのやりとりである。

図４および図５は、前述のように、それぞれ通信装置１０２－１からセッション制御サーバ１０１－１に送信する信号例、および通信装置１０２－１がセッション制御サーバ１０１－１から受信する信号例である。このため、本例において

は、セッション制御サーバ１０１－１から通信装置１０２－１に送信する信号例が図５、通信装置１０２－１から受信する信号例が図４となる。

図４に示すように、例えば、セッション制御サーバ１０１－１が通信装置１０２－１から受信した信号が、ＲＦＣ３２６１に準拠したＳＩＰメッセージの１つであるＲＥＧＩＳＴＥＲメソッドであり、そのメッセージに通信装置の位置情報が有効時間と共に設定されている（４０２）。また、公開鍵証明書要求およびユーザ認証キーも設定されている（４０２）。これらの情報は、機密性を保つために、暗号化鍵で暗号化されている。

セッション制御サーバ１０１－１は、コンテンツ暗号化鍵を取得するために、まず、暗号化されたコンテンツ暗号化鍵の復号化を行う。

復号化には、セッション制御サーバ１０１－１の秘密鍵を用いてもよいし、セッション制御サーバ１０１－１と通信装置１０２－１の使用者との間の事前共有鍵（パスワードなど）を用いてもよい。

セッション制御サーバ１０１－１は、復号化して取得したコンテンツ暗号化鍵を用いて、暗号化された情報の復号化を行う。

復号化して取得した位置情報登録要求、ユーザ認証キー、証明書発行要求を得る。

セッション制御サーバ１０１－１は、ユーザ認証後、証明書発行要求が正当であることを確認し、セッション制御サーバ１０１－１が発行元となる公開鍵証明書を発行する。

発行した公開鍵証明書の有効期限（５０４）は、位置情報の有効期限と同一に設定する。

位置情報と公開鍵証明書とを有効期限とともに記憶する。

セッション制御サーバ１０１－１は、図５に示すように、ＲＥＧＩＳＴＥＲメソッドに対する正常応答２００　ＯＫ（５００）に、登録された位置情報と、セッション制御サーバ１０１－１が認めた有効時間を共に設定する（５０４）。これらの情報は、機密性を保つために、暗号化鍵で暗号化する（５０２）。また、公開鍵証明書も設定する（５０６）。セッション制御サーバ１０１－１が信号を暗号化するには、まず暗号化鍵を生成する。次にその暗号化鍵を暗号化する。こ

のとき、通信装置１０２－１の公開鍵を用いてもよいし、セッション制御サーバ１０１－１と通信装置１０２－１の使用者との間の事前共有鍵(パスワードなど)を用いてもよい。

セッション制御サーバ１０１－１は、このように生成した信号を、通信装置１０２－１に送信する。

改竄有無の検出のために、セッション制御サーバ１０１－１のデジタル署名(５０３）を添付して送信してもよい。

図８は、第２の実施例に係る通信装置の位置登録と証明書発行処理とのフローチャートである。

通信装置から送信する信号について、暗号化または復号化などが行われるが、ここではその処理は記載を省略している。

まず、通信装置１０２－１は、通信装置１０２－１の位置登録要求を行うため、非対称鍵ペアを作成し、その鍵ペアの中の公開鍵に対する証明書発行要求と、位置登録要求とを一括した位置登録および証明書発行要求信号をセッション制御サーバ１０１－１に送信する（５１）（８－Ａ）なお、位置登録および証明書発行要求信号には、位置登録要求が含まれるが、証明書発行要求は含まれることもあれば含まれないこともある。セッション制御サーバ１０１－１は、この信号を受信し（５２）、セッション制御を行い（５３）、信号種別を判定して（５４）、位置登録要求であれば、位置登録要求を受信し（５５）、証明書発行要求があるか否かを判定し（５６）、証明書発行要求がなければ、位置情報および証明書を管理する（５９）。また、証明書発行要求があれば、証明書発行要求を受信し（５７）、証明書を発行し（５８）、位置情報および証明書を管理する（５９）。そして、セッション制御を行い（６０）、通信装置１０２－１に信号送信する（６１）（８－Ｂ）。通信装置１０２－１は、位置登録および証明書発行完了通知を受信する（６２）。なお、位置登録および証明書発行完了通知には、位置登録完了通知が含まれるが、証明書発行完了通知は含まれることもあれば含まれないこともある。

（第３の実施例）

第３の実施例として、他のセッション制御サーバ１０１－２が通信装置１０２－２から受信した信号が、ＳＩＰに準拠したＳＩＰメッセージの１つであるＯＰＴＩＯＮＳメソッドであって、そのメッセージに通信装置１０２－１の公開鍵証明書問合せ要求が設定されている場合のやりとりについて記載する。

図６は、図３のセッション制御サーバの受信信号例を示す図であり、図７は、同じくセッション制御サーバの送信信号例を示す図である。

６００には、問合せ内容の改竄の有無の検出を可能とするために、通信装置１０２－２のユーザのデジタル署名、ならびに署名検証のための通信装置１０２－２のユーザの公開鍵証明書が設定されている（６０４）。セッション制御サーバ１０１－２は、ＯＰＴＩＯＮＳメソッドのＲｅｑｕｅｓｔ－ＵＲＩに設定されているドメイン名を参照して、自ドメイン宛のメソッドか否かを判定する。自ドメイン宛でない場合には、ドメイン名として示されるセッション制御サーバ１０１－１に送信する。

セッション制御サーバ１０１－１は、ＯＰＴＩＯＮＳメソッドを受信して、ＯＰＴＩＯＮＳメソッドのＲｅｑｕｅｓｔ－ＵＲＩに設定されているドメイン名を参照して、自ドメイン宛のメソッドか否かを判定する。自ドメイン宛のメソッドであれば、証明書登録要求であるか否かを判別する。証明書登録要求であれば、位置情報および公開鍵証明書記憶手段１２６において、通信装置１０２－１のユーザの位置情報、公開鍵証明書および有効時間を検索し、その時点で有効な情報を取得する。それらを取得した情報を、図７に示す、ＯＰＴＩＯＮＳメソッドに対する応答２００　ＯＫに設定して、通信装置１０２－２に送信する。

セッション制御サーバ１０１－１は、このメッセージを通信装置１０２－２に直接送信することもできるが、ここではセッション制御サーバ１０１－２を経由して送信する。

図９は、本発明の第３の実施例に係る証明書問い合せ処理のフローチャートである。通信装置から送信する信号について、暗号化または復号化などが行われるが、ここではその処理は記載を省略している。

通信装置１０２－２は、証明書問合せ要求信号をセッション制御サーバ１０１－２に送信する（８１）（９－Ａ）。セッション制御サーバ１０１－２は、この

信号を受信すると（８２）、セッション制御を行い（８３）、自ドメイン宛か否かを判定し（８４）、自ドメイン宛でなければ、セッション制御を行って（８９）、該当するセッション制御サーバに送信する（９０）。この場合、宛先であるセッション制御サーバ１０１－１に転送する（９－Ｂ）。自ドメイン宛であれば、信号種別を判定し（８５）、証明書問合せ要求であれば、証明書問合せ要求を受信し（８６）、証明書があるか否かを判定し（８７）、証明書があれば、証明書の通知を行い（８８）、セッション制御を行って（８９）、通信装置１０２－２に信号送信する（９０）（９－Ｄ）。

セッション制御サーバ１０１－１は、その信号を受信し（９１）、セッション制御を行い（９２）、自ドメイン宛であるか否かを判定し（９３）、自ドメイン宛でなければ、セッション制御を行って（９８）、他のセッション制御サーバに送信するか（９９）、送信すべき宛先が不明であれば、エラー応答をセッション制御サーバ１０２－１に返却する。自ドメイン宛であれば、信号種別を判定し（９４）、証明書問合せ要求であれば、証明書問合せ要求を受信する（９５）。証明書があるか否かを判定し（９６）、証明書があれば、証明書通知を行い（９７）、セッション制御を行って（９８）、セッション制御サーバ１０１－２に信号送信する（９９）（９－Ｃ）。

セッション制御サーバ１０１－２は、この信号を受信すると（８２）、セッション制御を行い（８３）、自ドメイン宛でないので、宛先である通信装置１０２に信号を送信する（９０）（９－Ｄ）。通信装置１０２－２は、この証明書通知を受信する（８０）。

セッション制御サーバ１０１－２は、エラー応答を受信すると、通信装置１０２－２に該エラー応答を送信する。

このように、本実施形態に係る通信方法では、通信装置で利用可能な状態となっている公開鍵証明書をセッション管理サーバで管理することで、セッション通信で利用可能な電子証明書（公開鍵証明書）の配布・流通が可能となる。

また、セッション制御サーバによる電子証明書の配布時に、セッション制御サーバによって証明書の有効性が確認されているため、セッション制御信号内で使

用する電子証明書の有効性を、認証局などに問い合せることなく確認することが可能となる。

なお、図８および図９の動作フローをプログラム化した後、これらのプログラムをＣＤ－ＲＯＭなどの記録媒体に格納しておけば、プログラムの販売や貸与の場合に便利である。また、セッション制御サーバとなるコンピュータや、通信装置のコンピュータにこの記録媒体を装着して、プログラムをインストールし、プログラムを実行させることにより、本発明を容易に実現することができる。

以上説明したように、本発明の第１実施形態によれば、通信装置間の機密性の高い信号送受信のために必要な電子証明書（公開鍵証明書）を、セッション制御サーバが通信装置対応の有効性を確認した上で、これを管理するので、実利用可能な電子証明書の配布が可能であり、ユーザへのセッション確立時の有効性確認が容易となる。

（第２の実施形態）

［システム構成］

図１０は、本発明の第２の実施形態に係る通信システムの構成図である。

図１０に示すように、本通信システム２００は、複数のセッション制御サーバ２０１と、複進の通信装置２０２とＮＡＴ／ファイヤウォール装置２０３、およびネットワーク２０を含むように構成される。

なお、通信装置２０２は、本発明による手順に従いセッション制御サーバ２０１を介して暗号化情報を含む信号により通信を行う。なお、通信システム２００においては、セッション制御サーバ２０１は２台に限定されるものではない。ここでは、通信装置２０２が２台示されているが、２台に限定されるものではない。ＮＡＴ／ファイヤウォール装置２０３が１台示されているが、１台に限定されるものではない。

なお、本発明によれば、通信装置２０２はパソコン、携帯端末、あるいはゲートウェイなどの通信機器を含み、ネットワーク２０の構成は、有線、無線を問わない。以降は、説明の便宜を図るため、通信装置２０２－１を発信側とし、通信装置２０２－２を着信側として説明する。また、セッション制御サーバ２０１－１を発信側、セッション制御サーバ２０１－２を着信側として説明する。

通信装置２０２－１が、暗号化情報とともに、通信装置２０２－２用に暗号化した第一の暗号化鍵とセッション制御サーバ２０１－１用に暗号化した第一の暗号化鍵を、セッション制御サーバ２０１－１に送信する。

セッション制御サーバ２０１－１は、通信装置２０２－１から送信された暗号化情報と２つの暗号化した第一の暗号化鍵とを受信し、これらのうちセッション制御サーバ用情報を復号化し、得られた第一の暗号化鍵で暗号化情報を復号化する。このように、情報の参照が可能となる。

この際、セッション制御サーバ２０１－１は、参照した情報をもとにＮＡＴ／ファイヤウォール装置２０３に対して、フィルタリング条件の変更要求を送信してもよい。ＮＡＴ／ファイヤウォール装置２０３からフィルタリング条件の変更完了通知を受信した後、セッション制御サーバ２０１－１は、通信装置２０２－１から受信した暗号化情報を含む信号と２つの第一の暗号化鍵とを、セッション制御サーバ２０１－２に送信する。

セッション制御サーバ２０１－２は、セッション制御サーバ２０１－１から送信された暗号化情報と２つの暗号化した第一の暗号化鍵とを受信するが、これらを復号化できないため、暗号化された情報を参照できない。セッション制御サーバ２０１－２は、受信した暗号化情報と２つの暗号化した第一の暗号化鍵とを通信装置２０２－２に送信する。

通信装置２０２－２は、セッション制御サーバ２０１－２から受信した通信装置２０２－２用情報を復号化し、得られた第一の暗号化鍵で暗号化した情報を復号化する。このように、情報の参照が可能となる。

通信装置２０２－２は、通信装置２０２－１に送信すべき応答信号などの信号をセッション対応に記憶している第一の暗号化鍵を再利用して暗号化し、セッション制御サーバ２０１－１，２０１－２経由で、あるいは直接、通信装置２０２－１に送信する。

［通信装置］

図１２は、本発明の第２の実施形態に係る通信装置のブロック構成図である。

図１２に示すように、通信装置２０２は、信号送信手段２２０、セッション制御手段２２１、暗号化鍵生成手段２２２、暗号化鍵暗号化手段２２３、信号情報

暗号化手段２２４、暗号化鍵再利用手段２２５、信号情報復号化手段２２６、暗号化鍵復号化手段２２７、信号受信手段２２８、暗号化鍵更新手段２２９を含むように構成される。

通信装置２０２－１は、セッション制御手段２２１で生成された信号のうち、機密性が必要な情報を、暗号化鍵生成手段２２２で生成された第一の暗号化鍵を使用して、信号暗号化手段２２４で暗号化する。

そして、その第一の暗号化鍵を、開示先通信装置およびサーバの第二の暗号化鍵（例えば、実施形態においては公開鍵とする）を使用して、暗号化鍵暗号化手段２２３によって各々暗号化する。その際に、使用した第一の暗号化鍵は、暗号化鍵再利用手段２２５にセッション識別子に対応付けて記憶される。

セッション制御手段２２１で生成された情報のうち、暗号化していない情報に、セッション制御サーバ２０１および送信先通信装置に復号化を要求する情報を追加し、第一の暗号化鍵で暗号化した情報と、復号化要求対象が保持する第二の暗号化鍵により暗号化した第一の暗号化鍵とともに、信号送信手段２２０によって、セッション制御サーバ２０１－１に送信する。これにより、機密性が必要な情報について、特定のセッション制御サーバ２０１－１と通信装置２０２－２に対してのみ開示可能な状態で信号を送信することが可能となる。

図１３は、本発明の第２の実施形態に係る通信装置２０２－１の送信信号例を示す図である。

通信装置２０２－１は、機密性が必要な情報を第一の暗号化鍵を使用して暗号化する。その第一の暗号化鍵を、開示先通信装置およびサーバの各々の第二の暗号化鍵を使用して各々暗号化する。暗号化していない情報に、セッション制御サーバ２０１に対して復号化を要求する情報を追加する。第一の暗号化鍵で暗号化した情報と、復号化要求対象が保持する第二の暗号化鍵により暗号化した第一の暗号化鍵とともに、信号送信手段２２０によって、セッション制御サーバ２０１－１に送信する。

この送信信号例については、さらに、第４の実施例の説明で図１５を参照して説明する。

図１４は、本発明の第２の実施形態に係る通信装置２０２－２の送信信号例を示す図である。

この送信信号例については、さらに、第４の実施例の説明で、図１５を参照して説明する。

[セッション制御サーバ]

図１１は、本発明の第２の実施形態に係るセッション制御サーバのブロック構成図である。

図１１に示すように、セッション制御サーバ２０１は、信号受信手段１１０、復号化判断手段２１１、暗号化鍵復号化手段２１２、復号化鍵再利用手段２１３、信号情報復号化手段２１４、セッション制御手段２１５、信号送信手段２１６を具備している。ＮＡＴ／ファイヤウォール制御手段２１７、主情報通信受信手段２１８、主情報復号化手段２１９を具備している。

暗号化鍵復号化手段２１２は、第一の暗号化鍵の格納されたデータを参照して、どの第二の暗号化鍵に対応した第二の復号化鍵を使用して、復号化するかを判断した上で、第一の暗号化鍵の復号化を行い、情報復号化手段２１４に復号化鍵を渡す。信号情報の復号化により、通信装置間の制御情報が参照可能となり、セッション制御手段２１５に必要な情報が提供される。

復号化鍵は、セッション制御手段２１５内の識別子に対応して、復号化鍵再利用手段２１３において、信号情報に含まれるセッションの識別子に対応して、復号化鍵を記憶する。

セッション制御手段２１５で信号送信の準備が整うと、信号受信手段１１０で受信した暗号化した情報と、暗号化した第一の暗号化鍵を含む信号を、信号送信手段２１６により通信装置２０２－２に送信する。

（第４の実施例）

図１５は、本発明の第４の実施例に係る通信方法の説明図である。

第４の実施例として、通信装置２０２－１で生成したセッション制御信号が、通信装置２０２－１から信頼されるセッション制御サーバ２０１－１、信頼されないセッション制御サーバ２０１－２経由で通信装置２０２－２に送信される例を説明する。

例えば、図１３に示すように、通信装置２０２－１からの送信信号は、ＲＦＣ３２６１に準拠したＳＩＰメッセージの１つであるＩＮＶＩＴＥメソッド８００であって、そのメッセージは、通信装置間の制御情報（ＳＤＰ：Ｓｅｓｓｉｏｎ Ｄｅｓｃｒｉｐｔｉｏｎ Ｐｒｏｔｏｃｏｌ）８０５が暗号化されて含まれている。ＳＤＰには、通信装置２０２－１の主情報通信の情報として、受信用ＩＰアドレス、ポート番号などを含む。改竄の検出のために、暗号化情報８０５に、通信装置２０２－１のユーザのデジタル署名を添付してもよい。

ＳＩＰメッセージは、セッション制御サーバ２０１－１、および、セッション制御サーバ２０１－２を経由して、通信装置２０２－２に送信される。暗号化した情報は、Ｓ／ＭＩＭＥのＥｎｖｅｌｏｐｅｄ－Ｄａｔａ８０４として設定する。その暗号化に使用した鍵（第一の暗号化鍵）は、セッション制御サーバ２０１の公開鍵と、着ユーザの公開鍵（第二の暗号化鍵）とで各々暗号化し、Ｅｎｖｅｌｏｐｅｄ－Ｄａｔａの中のｒｅｃｉｐｉｅｎｔＩｎｆｏｓ８０６として設定する。

また、第一の暗号化鍵は、セッション制御サーバ２０１－１と通信装置２０２－１と間の事前共有鍵や、通信装置２０２－１と通信装置２０２－２とのユーザ間の事前共有鍵によって、各々暗号化されてもよい。

そして、ＳＩＰメッセージ内の暗号化していない範囲８０１に、セッション制御サーバに復号化要求を示す値と、復号化すべきコンテンツＩＤとを含む。

ＳＩＰメッセージの一部８０１とＥｎｖｅｌｏｐｅｄＤａｔａ８０４とを合わせた情報８０２に対して、改竄有無の検出のために、通信装置２０２－１のユーザのデジタル署名８０３を添付してもよい。

セッション制御サーバ２０１－１は、通信装置２０２－１から送信されたＩＮＶＩＴＥメソッド８００を信号受信手段２１０によって受信する。復号化判断手段２１１において、復号化要求パラメータ（例：Ｓｅｓｉｏｎ－Ｐｏｌｉｃｙ）の値によって復号化要求を判断するか、暗号化された第一暗号化鍵が設定されたｒｅｃｉｐｉｅｎｔＩｎｆｏｓ８０６の復号化の可否によって復号化要求を判断してもよい。

復号化要求がある場合、暗号化鍵復号化手段２１２は、指定されたコンテンツＩＤの示すデータ８０４の中の、第一の暗号化鍵の格納されたデータ（ｒｅｃｉｐ

ｉｅｎｔＩｎｆｏｓ）８０６の型を参照して、どの第二の暗号化鍵に対応した第二の復号化鍵を使用して復号化するかを判断した上で、第一の暗号化鍵の復号化を行い、信号復号化手段２１４に復号化鍵を渡す。暗号化情報８０５の復号化により、通信装置間制御用の信号が参照可能となり、セッション制御手段２１５に必要な情報が提供される。

復号化要求がない場合や、指定されたコンテンツＩＤが設定されていない場合は、復号化処理は行わない。

セッション制御サーバ２０１－１は、復号化要求の有無にかかわらず、セッション制御手段２１５において、通信装置２０２－１から受信したＩＮＶＩＴＥメソッドについて、処理（必要なパラメータ変更など）を行い、信号送信手段２１６よってセッション制御サーバ２０１－２にこのＩＮＶＩＴＥメソッドを送信する。

セッション制御サーバ２０１－２は、セッション制御サーバ２０１－１から送信されたＩＮＶＩＴＥメソッドを信号受信手段２１０にて受信する。

復号化判断手段２１１において、復号化要求パラメータ（例：Ｓｅｓｉｏｎ－Ｐｏｌｉｃｙ）の値によって復号化要求を判断するか、あるいは暗号化された第一暗号化鍵が設定されたｒｅｃｉｐｉｅｎｔＩｎｆｏｓ８０６の復号化の可否によって復号化要求を判断してもよい。

復号化要求がないか、あるいは復号化不可な場合は、暗号化された通信装置間の制御情報は参照できない。セッション制御手段２１５によって参照可能な情報をもとに、ＩＮＶＩＴＥメソッドに対する処理（必要なパラメータの参照など）を行い、信号送信手段２１６よって通信装置２０２－１にＩＮＶＩＴＥメソッドを送信する。

信号を受信した通信装置２０２－２は、信号受信手段２２８で受信した信号の情報が第一の暗号化鍵で暗号化されており、第一の暗号化鍵が暗号化されて添付されている場合は、自身の第二の暗号化鍵に対応する第二の復号化鍵（第一の暗号化鍵が公開鍵の場合は秘密鍵、あるいは第二の暗号化鍵が事前共有鍵であれば同事前共有鍵）を使用して、暗号化鍵復号化手段２２７によって復号化し、第一の暗号化鍵を得る。その第一の暗号化鍵を使用して、暗号化された情報を信号復

号化手段２２６によって復号化し、情報が参照可能となる。その情報がセッション制御手段２２１に提示される。

セッション制御手段２２１は、必要に応じて送信すべき情報を生成するとともに、暗号鍵を暗号化鍵再利用手段２２５に、セッション識別子と対応付けて記憶する。

例えば、セッション制御手段２２１は、図１４に示すようなＩＮＶＩＴＥメソッドに対する応答信号として２００　ＯＫ　９００を送信する。送信すべき情報について、記憶している第一の暗号化鍵を使用して、信号暗号化手段２２４によって暗号化した情報９０５をＥｎｃｒｙｐｅｄ－Ｄａｔａ９０４として設定し、信号送信手段２２０によって信号を送信する。

また、改竄有無の検出のために、暗号化した情報９０５に対してデジタル署名を添付してもよい。

（応用例１：請求項２１参照）

その後のセッションの継続信号、例えばＭＥＳＳＡＧＥメソッドが、通信装置２０２－１からセッション制御サーバ２０１－１，２０１－２経由で通信装置２０２－２に送信される。通信装置２０２－１は、セッション単位に記録している第一暗号化鍵を使用して、ＭＥＳＳＡＧＥメソッドに設定するインスタントメッセージの内容を暗号化する。通信装置２０２－１は、第一暗号化鍵を添付しないで、暗号化した情報を含むＭＥＳＳＡＧＥメソッドを送信する。

当該信号を受信した通信装置２０２－２は、暗号化鍵再利用手段２２３において、セッション識別子をキーに用いて記憶している第一暗号化鍵を取得し、その第一暗号化鍵によって暗号化情報を復号化する。

（応用例２：請求項１８参照）

セッション制御サーバ２０１－１においても、セッション単位に記憶している第一の暗号化鍵を使用して暗号化情報を復号化する。

（応用例３：請求項２１参照）

一定時間経過後、通信装置２０２－１が、セッション制御サーバ２０１－１，２０１－２経由で通信装置２０２－２にＭＥＳＳＡＧＥメソッドを送信する際、暗号化鍵更新手段２２９によって第一暗号化鍵を更新する。通信装置２０２－１

は、更新した暗号化鍵を用いて情報を暗号化し、Ｓ／ＭＩＭＥのＥｎｖｅｌｏｐｅｄ－Ｄａｔａとして設定する。

通信装置２０２－１は、暗号化に使用したこの鍵（更新した第一の暗号化鍵）を、セッション制御サーバの公開鍵と、着ユーザの公開鍵（第二の暗号化鍵群）とで各々暗号化し、Ｅｎｖｅｌｏｐｅｄ－Ｄａｔａの中のｒｅｃｉｐｉｅｎｔＩｎｆｏｓとして設定する。

更新した第一の暗号化鍵を添付した暗号化情報を含む信号を受信した通信装置２０２－２は、更新された第一の暗号化鍵を暗号化鍵再利用手段２２５に記憶する。

（応用例４：請求項２３参照）

更新した第一の暗号化鍵を添付した暗号化情報を含む信号を受信したセッション制御サーバ２０１－１は、更新された第一の暗号化鍵を、暗号化鍵再利用手段２１３に記憶する。

（第５の実施例）

図１６は、本発明の第５の実施例に係る通信方法の説明図である。

本例では、セッション制御サーバが、セッション確立中に得られた情報を基にＮＡＴ／ファイヤウォール装置２０３のフィルタリング条件を変更する例を示している。

例えば、セッション制御サーバが通信装置２０２－１から受信した信号が、ＲＦＣ３２６１に準拠したＳＩＰメッセージの１つであるＩＮＶＩＴＥメソッドであって、そのメッセージに含まれる通信装置間の制御情報（ＳＤＰ：Ｓｅｓｓｉｏｎ　Ｄｅｓｃｒｉｐｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）が暗号化されている場合を考える。

第二の暗号化鍵に対応する第二の復号化鍵を使用して復号化することにより、制御情報に設定されている通信装置２０２－１の主情報通信経路のＩＰアドレスおよびポート番号などが参照可能となる。この情報を基に、ＮＡＴ／ファイヤウォール制御手段２１７において、遠隔のＮＡＴ／ファイヤウォール装置２０３に対してフィルタリング条件の変更（不特定ＩＰアドレスから特定ＩＰアドレスおよびポート番号宛のパケット通過指示）を要求する。

その後、通信装置２０２－２から受信した信号が、ＳＩＰメッセージの１つである２００　ＯＫ　応答であって、そのメッセージには通信装置間の制御情報（ＳＤＰ）が暗号化されて含まれている。復号化鍵再利用手段２１３に記憶していた第一の暗号化鍵を用いて暗号化情報を復号化して、通信装置２０２－２の主情報通信径路のＩＰアドレスおよびポート番号などの通信装置間の制御情報が参照可能となる。この情報を基に、ＮＡＴ／ファイヤウォール制御手段２１７において、遠隔のＮＡＴ／ファイヤウォール装置２０３に対してフィルタリング条件の変更（特定ＩＰアドレスから特定ＩＰアドレスおよびポート番号宛のパケット通過指示）を要求する。これにより、ＮＡＴ／ファイヤウォール装置２０３において、通信装置２０２－１と通信装置２０２－２間の主情報についてパケット通過が可能となる。

その後、セッション制御サーバ２０１－１が、通信装置２０２－１あるいは２０２－２が送信したＳＩＰメッセージの切断信号であるＢＹＥメソッドを受信すると、ＮＡＴ／ファイヤウォール制御手段２１７によって、ＮＡＴ／ファイヤウォール装置２０３に対してフィルタリング条件の変更（指定ＩＰアドレスから指定ＩＰアドレスおよびポート番号宛のパケット不通過指示）を要求する。

本実施形態で示したように、通信装置より信号内の情報を安全に開示されたセッション制御サーバ２０１－１により、セッション単位にＮＡＴ／ファイヤウォール制御を行うことができるので、アクセス制御の精度を高めることが可能となる。情報を開示されないセッション制御サーバ２０１－２は、主情報の経路情報が参照できないため、主情報のモニタが困難となり、その結果、主情報通信の機密性を高めることができる。

（第６の実施例）

図１７は、本発明の第６の実施例に係る通信方法の説明図である。

本例においては、セッション制御サーバ２０１－１が、セッション確立中に得られた情報を基に、暗号化された主情報についても通信記録が可能となる例を説明する。

例えば、通信装置２０２－１からの送信信号は、ＲＦＣ３２６１に準拠したＳＩＰメッセージの１つであるＩＮＶＩＴＥメソッドであって、そのメッセージに

通信装置情報ＳＤＰが暗号化されて含まれている。ＳＤＰには、通信装置２０２－１と通信装置２０２－２との間の主情報通信に使用するＩＰアドレス、ポート番号に加えて、主情報暗号化のための鍵情報が含まれる。

セッション制御サーバ２０１－１は、主情報通信記録の手段（受信手段２１８）と、主情報復号化手段２１９とを備え、遠隔のＮＡＴ／ファイヤウォール装置２０３に対して指示を送信する。

この指示は、前述の第５の実施例で説明したフィルタリング条件変更要求に加えて、主情報転送を指示する。セッション制御サーバ２０１－１の主情報通信受信手段２１８において、ＮＡＴ／ファイヤウォール装置２０３から主情報を受信する。主情報が暗号化されている場合、既に取得済みの主情報暗号化の鍵情報を用いて、主情報復号化手段２１９において復号化を行う。

復号化が正常終了すると、復号化された主情報、あるいは、暗号化された状態の主情報とその鍵情報とを記録する。

セッション制御サーバ２０１－２は、暗号化情報を復号化できないため、通信装置情報ＳＤＰを参照できず、ＳＤＰに含まれる主情報暗号化のための鍵情報を参照できない。そのため、ネットワーク内のモニタ装置で主情報をモニタしても、主情報が暗号化されており復号化することができない。

このように、主情報が暗号化されている場合でも、セッション制御サーバによる復号化した主情報の記録が行えるため、通信情報の監査、および、記録が可能となる。

なお、第４～第６の実施例で説明した処理順序をプログラム化して、ＣＤ－ＲＯＭなどの記録媒体に格納しておけば、プログラムの販売や貸与の際に便利である。また、セッション制御サーバ２０１－１，２０１－２のコンピュータに記録媒体を装着して、プログラムをインストールし、これを実行させることで、本発明を容易に実現することができる。

このように、本実施形態に係る通信システムは、通信装置間だけでなく、信号中継を行うセッション制御サーバに対しても情報開示が可能であるため、通信装置が送受信する伝達信号の機密性を高めながら、特定のセッション制御サーバによる通信制御が可能となる。

以上説明したように、本発明の第２実施形態によれば、通信装置間の機密性の高い信号送受信を保証した上で、通信装置の要求に応じて特定のセッション制御サーバに対してのみ信号情報を開示することが可能である。また、通信装置間の接続構成によらず、信号情報を開示するセッション制御サーバの指定が可能となる。

（第３の実施形態）

［システム構成］

図１８は、本発明の第３の実施形態に係る通信システムの構成図である。

図１８に示すように、通信システム３００は、ネットワーク３０を介して通信可能に接続された複数のセッション制御サーバ３０１と、複数の通信装置３０２と、ＮＡＴ／ファイヤウォール装置３０３と、ネットワーク３０とを含むように構成される。

また、通信装置３０２は、本発明による手順に従ってセッション制御サーバ３０１を介して暗号化信号により通信を行う。なお、通信システム３００においては、セッション制御サーバ３０１は２台示されているが、２台に限定されるものではない。また、通信装置３０２が２台示されているが、これも２台に限定されるものではない。また、ＮＡＴ／ファイヤウォール装置３０３が１台示されているが、これも１台に限定されるものではない。

なお、本発明においては、通信装置３０２は、パソコン、携帯端末、ゲートウェイなどの通信機器を含み、ネットワーク３０の構成は有線、無線を問わない。

これ以降は、説明の便宜を図るために、通信装置３０２－１を発信側とし、通信装置３０２－２を着信側として説明する。

通信装置３０２－１が、暗号化信号とともにセッション制御サーバ３０１－１用第二の暗号化鍵で暗号化した第一の暗号化鍵を、セッション制御サーバ３０１－１に送信する。セッション制御サーバ３０１－１が、通信装置３０２－１から送信された暗号化信号と暗号化した第一の暗号化鍵を受信して、セッション制御サーバ３０１－１用第二の暗号化鍵に対応する復号化鍵で、第一の暗号化鍵を復号化し、その第一の暗号化鍵で暗号化信号を復号化することにより、信号の参照および／または変更が可能となる。

セッション制御サーバ３０１－１は、受信した第一の暗号化信号（あるいは新規に作成した第一の暗号化信号）を使用して情報を暗号化し、暗号化に使用した第一の暗号化鍵を、通信装置３０２－２用の第二の暗号化鍵で暗号化し、セッション制御サーバ３０１－２に送信する。

セッション制御サーバ３０１－２は、セッション制御サーバ３０１－１から送信された暗号化信号と第一の暗号化鍵を受信する。しかし、これらを復号できないため、暗号化された情報は参照できない。セッション制御サーバ３０１－２は、受信した暗号化信号と暗号化した第一の暗号化鍵を、通信装置３０２－２に送信する。

通信装置３０２－２は、セッション制御サーバ３０１－２から受信した通信装置３０２－２用第二の暗号化鍵に対応する復号化鍵で、第一の暗号化鍵を復号化し、その第一の暗号化鍵で暗号化信号を復号化することにより、情報の参照が可能となる。

通信装置３０２－２は、通信装置３０２－１に送信すべき応答信号などの信号を、復号化した暗号化鍵を再利用して暗号化し、セッション制御サーバ３０１－２、セッション制御サーバ３０１－１経由で通信装置３０２－１に送信する。

［通信装置］

図２０は、本発明の第３の実施形態に係る通信装置のブロック構成図である。

図２０に示すように、通信装置３０２は、信号送信手段３２０、セッション制御手段３２１、暗号化鍵生成手段３２２、暗号化鍵暗号化手段３２３、信号暗号化手段３２４、暗号化鍵再利用手段３２５、信号復号化手段３２６、暗号化鍵復号化手段３２７、信号受信手段３２８、および暗号化鍵更新手段３２９を含むように構成される。

通信装置３０２－１は、セッション制御手段３２１で生成された信号のうち、機密性が必要な信号を暗号化鍵生成手段３２２で生成された暗号化鍵を使用して、信号暗号化手段３２４で暗号化する。

そして、その第一の暗号化鍵を開示先である特定のセッション制御サーバの公開鍵を使用して、暗号化鍵暗号化手段３２３により各々暗号化する。その際に、

使用した暗号化鍵は、暗号化鍵再利用手段３２５にてセッションと対向装置に対応させて記憶する。

セッション制御手段３２１で生成された信号のうち、暗号化していない信号に、セッション制御サーバに復号化を要求する情報を追加し、暗号化した信号と、暗号化した暗号化鍵とともに、信号送信手段３２０にてセッション制御サーバ３０１－１に送信する。これにより、機密性が必要な情報について、特定のセッション制御サーバ３０１－１に対してのみ開示可能な状態で、信号送信が可能となる。

図２１は、本発明の第３の実施形態に係る通信装置３０２－１の送信信号例の図である。

通信装置３０２－１からの送信信号は、ＲＦＣ３２６１に準拠したＳＩＰメッセージの１つであるＩＮＶＩＴＥメソッドであって、そのメッセージにおいて通信装置間の制御情報（ＳＤＰ：Ｓｅｓｓｉｏｎ Ｄｅｓｃｒｉｐｔｉｏｎ Ｐｒｏｔｏｃｏｌ）１００５が暗号化されて含まれている。ＳＤＰには、通信装置３０２－１の主情報通信の情報として、受信用ＩＰアドレス、ポート番号などが含まれる。改竄有無の検出のために、暗号化情報１００５には通信装置３０２－１のユーザのデジタル署名を添付してもよい。暗号化された情報は、Ｓ／ＭＩＭＥのＥｎｖｅｌｏｐｅｄ－Ｄａｔａ１００４として設定されている。その暗号化に使用した鍵（第一の暗号化鍵）は、セッション制御サーバの公開鍵（第二の暗号化鍵）で暗号化され、Ｅｎｖｅｌｏｐｅｄ－Ｄａｔａの中のｒｅｃｉｐｉｅｎｔＩｎｆｏｓ１００６として設定される。ＳＩＰメッセージ内の暗号化していない範囲１００１に、セッション制御サーバに復号化要求を示す値と、復号化すべきＣｏｎｔｅｎｔ－ＩＤとが含まれる。

ＳＩＰメッセージの一部１００１とＥｎｖｅｌｏｐｅｄＤａｔａ１００４とを合わせた情報１００２に、改竄有無の検出のために、デジタル署名１００３を添付してもよい。

図２２は、本発明の第３の実施形態に係る通信装置３０２－２の送信信号例の図である。

通信装置３０２－２は、ＩＮＶＩＴＥメソッドに対する応答信号として２００ＯＫ１１００を送信する。通信装置３０２－２は、暗号化された情報１１０５を

送信する。改竄有無の検出のために、暗号化された情報１１０５にデジタル署名をしてもよい。また、ＳＩＰメッセージの一部１１０１とＥｎｖｅｌｏｐｅｄＤａｔａ１１０４とを合わせた情報１１０２に、デジタル署名１１０３が添付されてもよい。

[セッション制御サーバ]

図１９は、本発明の第３の実施形態に係るセッション制御サーバのブロック構成図である。

図１９に示すように、セッション制御サーバ３０１は、信号受信手段３１０、復号化判断手段３１１、暗号化鍵復号化手段３１２、復号化鍵再利用手段３１３、信号復号化手段３１４、セッション制御手段３１５、暗号化鍵生成手段３１６、暗号化鍵暗号化手段３１７、信号暗号化手段３１８、信号送信手段３１９を備える。それに加えて、ＮＡＴ／ファイヤウォール制御手段３３０、主情報通信受信手段３３１、主情報復号化手段３３２を備えてもよい。

暗号化鍵復号化手段３１２は、信号復号化手段３１４の復号化鍵として第一の暗号化鍵を取得する手段を提供する。信号の復号化により、通信装置間の制御用の情報が参照可能となり、セッション制御手段３１５に必要な情報を提供する。

第一の暗号化鍵は、セッション制御手段３１５内のセッション識別子と対向装置識別子に対応付けて、復号化鍵再利用手段３１３に、復号化鍵が記憶される。セッション制御手段３１５で、復号化した情報を必要に応じて参照および／または変更する。セッション制御サーバ３０１は、第一の暗号化鍵をそのまま利用して、あるいは、暗号化鍵生成手段３１６で第一の暗号化鍵を新規に生成し、暗号化鍵暗号化手段３１７で次段の信頼できるセッション制御サーバあるいは通信装置３０２－２の第二の暗号化鍵（公開鍵あるいは事前共有鍵）を暗号化する。そして、第一の暗号化鍵をそのまま利用するか、あるいは暗号化鍵生成手段３１６で生成した新規の第一の暗号化鍵を使用して、情報を暗号化する。

このように生成した暗号化情報および暗号化した暗号化鍵を、信号送信手段３１９によって次段の信頼できるセッション制御サーバ、あるいは通信装置３０２－２に送信する。

（第７の実施例）

図２３は、本発明の第７の実施例に係る通信方法の説明図である。

ここでは、通信装置３０２－１が生成したセッション制御信号が、通信装置３０２－１から信頼されるセッション制御サーバ３０１－１に送信され、さらにセッション制御サーバ３０１－１からセッション制御サーバ３０１－２経由で通信装置３０２－２に送信される例を示している。

例えば、通信装置３０２－１からの送信信号は、ＲＦＣ３２６１に準拠したＳＩＰメッセージの１つであるＩＮＶＩＴＥメソッドであり、そのメッセージに含まれる通信装置間の制御情報（ＳＤＰ）が暗号化されているものとする（図２１の１００５参照）。ＳＤＰには、通信装置３０２－１の主情報通信の情報として、受信用ＩＰアドレス、ポート番号などが含まれる。

ＳＩＰメッセージは、セッション制御サーバ３０１－１およびセッション制御サーバ３０１－２を経由して、通信装置３０２－２に送信される。

情報の暗号化に使用された鍵（第一の暗号化鍵）は、セッション制御サーバの公開鍵（第二の暗号化鍵）で暗号化され、Ｅｎｖｅｌｏｐｅｄ－Ｄａｔａの中のｒｅｃｉｐｉｅｎｔＩｎｆｏｓ（図２１の１００６参照）として設定される。

また、第一の暗号化鍵は、セッション制御サーバ３０１－１と通信装置３０２－１の使用者との間の事前共有鍵（パスワードなど）で暗号化されてもよい。

セッション制御サーバ３０１－１は、通信装置３０２－１から送信されたＩＮＶＩＴＥメソッドを信号受信手段３１０によって受信する。復号化判断手段３１１において、復号化要求パラメータ（例：Ｓｅｓｓｉｏｎ－Ｐｏｌｉｃｙ）の値によって復号化要求を判断するか、あるいは、暗号化された第一暗号化鍵が設定されたｒｅｃｉｐｉｅｎｔＩｎｆｏｓ（図２１の１００５参照）の復号化の可否によって復号化要求を判断してもよい。

復号化要求がある場合には、暗号化鍵復号化手段３１２は、第一の暗号化鍵の格納されたデータ（ｒｅｃｉｐｉｅｎｔＩｎｆｏｓ）（図２１の１００６参照）の型を参照して、どの第二の暗号化鍵に対応した第二の復号化鍵で復号化するかを判断した上で、第一の暗号化鍵の復号化を行い、信号復号化手段３１４に復号化鍵を渡す。暗号化情報の復号化により、通信装置間制御情報が参照および／変更または可能となり、セッション制御手段３１５に必要な情報を提供する。必要

に応じて、セッション制御手段３１５にて通信装置間制御情報を変更する。次に、第一の暗号化鍵をそのまま利用するか、あるいは、暗号化鍵生成手段３１６にて新規に生成した第一の暗号化鍵を使用して、セッション制御手段３１５にて変更した後の情報を暗号化する。

第一の暗号化鍵は、通信装置３０２－１用の第二の暗号化鍵（公開鍵あるいは事前共有鍵）によって情報を暗号化する。セッション制御サーバ３０１－２が信頼できる場合には、セッション制御サーバ３０１－２用の第二の暗号化鍵で暗号化してもよい。セッション制御サーバ３０１－１は、セッション制御手段３１５において、通信装置３０２－１から受信したＩＮＶＩＴＥメソッドについて処理（必要なパラメータ変更など）を行い、信号送信手段３１９よってセッション制御サーバ３０１－２にＩＮＶＩＴＥメソッドを送信する。

セッション制御サーバ３０１－２は、セッション制御サーバ３０１－１から送信されたＩＮＶＩＴＥメソッドを信号受信手段３１０によって受信する。復号化判断手段３１１において、復号化要求パラメータ（例：Ｓｅｓｓｉｏｎ－Ｐｏｌｉｃｙ）の値によって復号化要求を判断するか、あるいは、暗号化された第一の暗号化鍵が設定されたｒｅｃｉｐｉｅｎｔＩｎｆｏｓ（図２１の１００６参照）の復号化の可否によって復号化要求を判断してもよい。

復号化要求がないか、あるいは復号化不可な場合は、セッション制御手段３１５によって、参照可能な情報をもとに、ＩＮＶＩＴＥメソッドに対する処理（必要なパラメータ変更など）を行い、信号送信手段３１９よって通信装置３０２－２にＩＮＶＩＴＥメソッドを送信する。

信号を受信した通信装置３０２－２は、信号受信手段３２８で受信した信号が暗号化されており、第一の暗号化鍵が暗号化されて添付されている場合は、自身の第二の暗号化鍵に対応する第二の復号化鍵（第一の暗号化鍵が公開の場合には秘密鍵、あるいは第一の暗号化鍵が事前共有鍵であれば同じ事前共有鍵）を使用して、暗号化鍵復号化手段３２７によって復号化し、第一の暗号化鍵を得る。その第一の暗号化鍵を使用して、暗号化された情報を信号復号化手段３２６によって復号化することにより、情報が参照可能となる。その情報がセッション制御手段３２１に提示される。

セッション制御手段３２１は、必要に応じて送信すべき情報を生成するとともに、暗号化鍵を暗号化鍵再利用手段３２５に、セッションおよび対向装置に対応付けて記憶する。例えば、セッション制御手段３２１は、ＩＮＶＩＴＥメソッドに対する応答信号として、図２２の１１００を送信する。送信すべき情報について、記憶している第一の暗号化鍵を使用して、信号暗号化手段３２４によって情報を暗号化し、信号送信手段３２０によって送信する。

（応用例５：請求項４２参照）

その後のセッションの継続信号が、例えばＭＥＳＳＡＧＥメソッドが通信装置３０２－１よりセッション制御サーバ３０１－１、３０１－２経由で通信装置３０２－２に送信される。通信装置３０２－１は、セッション単位に記録している第一の暗号化鍵を使用してＭＥＳＳＡＧＥメソッドに設定する情報を暗号化する。第一の暗号化鍵を添付しないで、暗号化した情報を含むＭＥＳＳＡＧＥメソッドを送信する。

当該信号を受信した通信装置３０２－２は、暗号化鍵再利用手段３２５において、セッションと対向装置の識別子をキーに、記憶している第一の暗号化鍵を取得し、その第一の暗号化鍵にて暗号化情報を復号化する。

（応用例６：請求項３８，３９参照）

セッション制御サーバ３０１－１においても、セッションと対向装置単位に記憶している第一の暗号化鍵を使用して暗号化情報を復号化する。

（応用例７：請求項４３参照）

また、一定時間経過後、通信装置３０２－１がＭＥＳＳＡＧＥメソッドをセッション制御サーバ３０１－１，３０１－２経由で通信装置３０２－２に送信する際に、暗号化鍵更新手段３２９にて第一の暗号化鍵を更新する。更新した暗号化鍵を用いて情報を暗号化し、Ｓ／ＭＩＭＥのＥｎｖｅｌｏｐｅｄ－Ｄａｔａとして設定する。

その暗号化に使用した鍵（更新した第一の暗号化鍵）は、セッション制御サーバの公開鍵（第二の暗号化鍵）で暗号化し、Ｅｎｖｅｌｏｐｅｄ－Ｄａｔａの中のｒｅｃｉｐｉｅｎｔＩｎｆｏｓとして設定する。

更新した第一の暗号化鍵を添付した暗号化信号を受信すると、通信装置３０２－２は、更新された第一の暗号化鍵を暗号化鍵再利用手段３２５にて記憶する。

（応用例８：請求項４５参照）

更新した第一の暗号化鍵を添付した暗号化信号を受信したセッション制御サーバ３０１－１は、更新された第一の暗号化鍵を暗号化鍵再利用手段３２５にて記憶する。

（第８の実施例）

図２４は、本発明の第８の実施例に係る通信方法の説明図である。

ここでは、セッション制御サーバ３０１－１が、セッション確立中に得られた情報を基にＮＡＴ／ファイヤウォール装置３０３のフィルタリング条件を変更する例を示している。

例えば、セッション制御サーバ３０１－１が通信装置３０２－１から受信した信号がＲＦＣ３２６１に準拠したＳＩＰメッセージの１つであるＩＮＶＩＴＥメソッドであって、そのメッセージに含まれる通信装置間の制御情報（ＳＤＰ）が暗号化されているとする。セッション制御サーバ３０１－１では、暗号化鍵復号化手段３１２において、第一の暗号化鍵の格納されたデータ（ｒｅｃｉｐｉｅｎｔＩｎｆｏｓ）（図２２の１００６参照）の型を参照して、どの鍵で復号化するかを判断した上で、第一の暗号化鍵の復号化を行う。

暗号化情報（図２２の１００５参照）を第一の暗号化鍵で復号化することで、通信装置間の制御情報（例えば、通信装置３０２－１の主情報通信径路のＩＰアドレスとポート番号）が参照可能および／または変更可能となる。

この情報を基に、ＮＡＴ／ファイヤウォール制御手段３３０において、遠隔のＮＡＴ／ファイヤウォール装置３０３に対してフィルタリング条件の変更（不特定ＩＰアドレスから特定ＩＰアドレスおよびポート番号宛のパケット通過指示）を要求する。また、セッション制御サーバ３０１－１は、主情報通信径路のＩＰアドレスおよびポート番号などの通信装置間の制御情報を変更することが可能である。

セッション制御サーバ３０１－１は、その後、通信装置３０２－２から受信した信号が、ＳＩＰメッセージの１つである２００　ＯＫ応答であって、そのメッ

セージに含まれる通信装置間の制御情報（ＳＤＰ）が暗号化されている。復号化鍵再利用手段３１３に記憶していた第一の暗号化鍵を用いて暗号化情報を復号化することで、通信装置３０２－２の主情報通信径路のＩＰアドレスおよびポート番号などの通信装置間の制御情報が参照可能となる。

この情報をもとに、ＮＡＴ／ファイヤウォール制御手段３３０において、遠隔のＮＡＴ／ファイヤウォール装置３０３に対して、フィルタリング条件の変更(特定ＩＰアドレスから特定ＩＰアドレスおよびポート番号宛のパケット通過指示)を要求する。これにより、ＮＡＴ／ファイヤウォール装置３０３において、通信装置３０２－１と通信装置３０２－２間の主情報についてパケット通過が可能となる。

その後、通信装置３０２－１あるいは３０２－２から受信したＳＩＰメッセージの切断信号であるＢＹＥメソッドを受信すると、セッション制御サーバ３０１－１は、ＮＡＴ／ファイヤウォール制御手段３３０において、ＮＡＴ／ファイヤウォール装置３０３に対してフィルタリング条件の変更（指定ＩＰアドレスから指定ＩＰアドレスおよびポート番号宛のパケット不通過指示）を要求する。

本実施例で示したように、通信装置より信号内の情報を安全に開示されたセッション制御サーバ３０１－１により、セッション単位にＮＡＴ／ファイヤウォール制御を行え、アクセス制御の精度を高めることが可能になる。情報を開示されないセッション制御サーバ３０１－２は、主情報の径路情報が参照できないため、主情報のモニタが困難となり、主情報通信の機密性を高めることができる。

（第９の実施例）

図２５は、本発明の第９の実施例に係る通信方法の説明図である。

ここでは、セッション制御サーバが、セッション確立中に得られた情報を基に、暗号化された主情報についても、通信記録が可能となる例を示している。

例えば、通信装置３０２－１からの送信信号は、ＲＦＣ３２６１に準拠したＳＩＰメッセージの１つであるＩＮＶＩＴＥメソッドであって、そのメッセージに含まれる通信装置情報ＳＤＰが暗号化されている。ＳＤＰには、通信装置３０２－１、通信装置３０２－２間の主情報通信の際に使用するＩＰアドレス、ポート番号に加えて、主情報暗号化のための鍵情報を含む。

セッション制御サーバ３０１－１が、主情報通信記録の手段１３１と、主情報復号化手段１３２を備え、遠隔のＮＡＴ／ファイヤウォール装置３０３に対して指示を送信する。

第８の実施例のフィルタリング条件変更要求に加えて、主情報転送を指示する。セッション制御サーバの主情報通信受信手段１３１にて、ＮＡＴ／ファイヤウォール装置３０３から主情報を受信する。主情報が暗号化されている場合には、既に取得済みの主情報暗号化の鍵情報を用いて、主情報復号化手段１３２にて復号化を行う。復号化が正常終了すると、その情報を記録する。

セッション制御サーバ３０１－２は、暗号化信号を復号化できないため、通信装置情報ＳＤＰは参照できず、ＳＤＰに含まれる主情報暗号化のための鍵情報は参照できない。そのため、ネットワーク内のモニタ装置で主情報をモニタしても、暗号化されており、それを復号化することができない。

このように、主情報が暗号化されている場合でも、特定の信頼できるセッション制御サーバによる復号化した主情報の記録が行え、通信情報の監査が可能となる。

このように、本実施例に係る通信方法では、任意の信号中継を行うセッション制御サーバに対して、情報開示／変更を可能にして、情報を安全に送信し、特定のセッション制御サーバによる通信制御が可能になる。

なお、上記第７、第８および第９の実施例で説明した手順をプログラム化し、そのプログラムをＣＤ－ＲＯＭなどの記録媒体に格納しておけば、プログラムの販売や貸与の場合に便利である。また、セッション制御サーバのコンピュータや、通信装置のコンピュータに記録媒体を装着して、プログラムをインストールし、実行させることで、本発明を容易に実現することができる。

以上説明したように、本発明によれば、接続構成によらず、特定のセッション制御サーバや着ユーザのみに、信号情報を開示させることが可能である。また、セッション制御サーバにより情報参照だけでなく、変更も可能である。

これにより、信頼できる宛先との間のセキュリティの確保が可能になるという顕著な効果を奏する。

請求の範囲

1．ネットワークを介してセッション制御サーバと通信可能に接続され、前記セッション制御サーバとの間で信号送受信を行うことによって他の通信装置とのセッションを確立する通信装置において、

非対称鍵ペアを作成する手段と、

前記セッション制御サーバに対して前記非対称鍵ペアのうちの公開鍵に対する証明書発行を要求する要求手段と、

該セッション制御サーバから公開鍵証明書発行完了の通知を受信する受信手段と、

受信した公開鍵証明書を記憶する記憶手段と、

該セッション制御サーバに対して該通信装置の位置の登録要求を送信する送信手段と、

該セッション制御サーバから有効期間を含む位置登録完了の通知を受信する受信手段とを備え、

前記位置登録要求と証明書発行要求とを一括した要求を送信する通信装置。

2．請求項1記載の通信装置において、

前記公開鍵証明書を記憶する記憶手段は、位置登録完了通知に含まれる有効期間を、発行された証明書の有効期間として記憶する通信装置。

3．ネットワークを介してセッション制御サーバと通信可能に接続され、前記セッション制御サーバとの間で信号送受信を行うことによって他の通信装置とのセッションを確立する通信装置において、

非対称鍵ペアを記憶する手段と、

前記非対称鍵ペアのうちの公開鍵の証明書を記憶する記憶手段と、

前記セッション制御サーバに対して該公開鍵証明書の登録要求を送信する送信手段と、

該セッション制御サーバに対して該通信装置の位置の登録要求を送信する送信手段と、

該セッション制御サーバから有効期間を含む位置登録完了の通知を受信する受信手段と

を備えた通信装置。

4．請求項3記載の通信装置において、

前記公開鍵証明書を記憶する記憶手段は、位置登録完了通知に含まれる有効期間を、発行された証明書の有効期間として記憶する通信装置。

5．ネットワークを介して複数の通信装置と通信可能に接続され、発信側の通信装置から送信された信号を受信し、受信された信号を着信側の通信装置に送信することによって、前記発信側の通信装置と前記着信側の通信装置とのセッションを確立させるセッション制御サーバであって、

前記通信装置からの位置登録要求と、公開鍵に対する証明書発行要求あるいは証明書登録要求とを一括した要求を受信する受信手段と、

前記要求を受け付け、公開鍵証明書の発行を行う、あるいは該公開鍵証明書の有効性を確認する手段と、

発行あるいは登録した該公開鍵証明書と位置情報とを、有効期間とともに記憶する手段と

を備えたセッション制御サーバ。

6．請求項5記載のセッション制御サーバにおいて、

前記公開鍵証明書の問い合せ要求を受信する受信手段と、

該公開鍵証明書の有効性を確認した上で、当該公開鍵証明書を通知する送信手段と

を備えたセッション制御サーバ。

7．ネットワークを介して通信可能に接続され、通信装置相互間でセッションを確立するための通信システムにおいて、

非対称鍵ペアを作成する手段、公開鍵に対する証明書発行の要求を行う要求手段、証明書発行通知を受信する受信手段、公開鍵証明書を記憶する記憶手段、位置登録要求を送信する送信手段、および有効期間を含む位置登録完了通知を受信する手段を備えた通信装置と、

前記通信装置からの位置登録要求を受信する受信手段、公開鍵に対する証明書発行あるいは証明書登録の要求を一括して受け付ける受信手段、証明書を発行あるいは証明書の有効性を確認する手段、および発行あるいは登録した証明書と位置情報とを、有効時間とともに記憶する記憶手段を備えたセッション制御サーバと

を有する通信システム。

8．請求項7記載の通信システムにおいて、

前記通信装置は、位置登録完了通知に含まれる有効期間を、発行された公開鍵証明書の有効期間として記憶する記憶手段とを備え、

前記セッション制御サーバは、証明書問い合せ要求を受信する受信手段と、証明書通知の送信手段とを備えた通信システム。

9．請求項7記載の通信システムにおいて、

前記通信装置は、非対称鍵ペアを記憶する手段と、公開鍵証明書の登録要求を送信する送信手段とを備え、

前記セッション制御サーバは、証明書問い合せ要求を受信する受信手段と、証明書通知の送信手段とを備えた通信システム。

10．ネットワークを介して通信可能に接続され、通信装置相互間でセッションを確立するための通信方法において、

セッション制御サーバは、通信装置から位置登録および証明書発行の要求信号を受信すると、信号種別を判定し、位置登録要求であれば、証明書発行要

求が含まれるか否かを判定し、前記信号に発行要求が含まれる場合には、証明書を発行して、該位置情報と該証明書とを管理するとともに、前記通信装置に対して位置情報および証明書発行完了通知の信号を送信する通信方法。

１１．ネットワークを介して通信可能に接続され、通信装置相互間でセッションを確立するための通信方法において、

セッション制御サーバは、通信装置から証明書問合せ要求信号を受信すると、セッション制御を行うとともに、自ドメイン宛てか否かを判定し、自ドメイン宛てであれば、信号種別を判定し、証明書問合せ要求であれば、証明書があるか否かを判定し、証明書があれば、該当する証明書を検索し、検索された証明書の有効性を確認して前記通信装置に対して証明書通知を送信し、自ドメイン宛てでない場合には、宛先のセッション制御サーバに該証明書問合せ要求信号を転送する通信方法。

１２．ネットワークを介して通信可能に接続され、通信装置相互間でセッションを確立するための通信用プログラムであって、

セッション制御サーバのコンピュータに、通信装置から位置登録および証明書発行の要求信号を受信する手順、信号種別を判定する手順、位置登録要求であれば、証明書発行要求が含まれるか否かを判定する手順、発行要求が含まれる場合には、証明書を発行する手順、該位置情報と該証明書とを管理する手順、および前記通信装置に対して位置情報と証明書発行完了通知の信号を送信する手順を実行させるための通信用プログラム。

１３．ネットワークを介して通信可能に接続され、通信装置相互間でセッションを確立するための通信用プログラムであって、

セッション制御サーバのコンピュータに、通信装置から証明書問合せ要求信号を受信する手順、セッション制御を行う手順、自ドメイン宛てか否かを判定する手順、自ドメイン宛てであれば、信号種別を判定する手順、証明書問合せ要求であれば、証明書があるか否かを判定する手順、証明書があれば、該当する

証明書を検索する手順、検索された証明書の有効性を確認する手順、前記通信装置に対して証明書通知を送信する手順、および自ドメイン宛てでない場合には、宛先のセッション制御サーバに該証明書問合せ要求信号を転送する手順を実行させるための通信用プログラム。

１４．請求項１２に記載の通信用プログラムを記録したコンピュータ読み取り可能な記録媒体。

１５．請求項１３に記載の通信用プログラムを記録したコンピュータ読み取り可能な記録媒体。

１６．ネットワークを介してセッション制御サーバと通信可能に接続され、１以上の前記セッション制御サーバを経由した他の通信装置との間で信号送受信を行うことによって該通信装置とのセッションを確立する通信装置において、

送信信号の守秘性を保持するために暗号化した情報を送信する際に、情報暗号化のための第一の暗号化鍵を生成する手段と、

該第一の暗号化鍵を用いて情報を暗号化する手段と、

該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する暗号化鍵暗号化手段と、

任意の第二の暗号化鍵で暗号化した第一の暗号化鍵を添付し、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、

前記暗号化鍵暗号化手段は、該第一の暗号化鍵を、送信先の通信装置または１以上の該セッション制御サーバの各々が保有する第二の暗号化鍵を用いて暗号化し、

前記送信手段は、暗号化された該第一の暗号化鍵と、該第一の暗号化鍵により暗号化された情報と、該セッション制御サーバに対する該情報の復号化要求指示とを送信する通信装置。

１７．ネットワークを介して複数の通信装置と他のセッション制御サーバと通信可能に接続され、発信側の通信装置あるいは他のセッション制御サーバから送信された信号を受信し、受信した信号を着信側の通信装置あるいは他のセッション制御サーバに送信することによって該発信側の通信装置と該着信側の通信装置とのセッションを確立させるセッション制御サーバにおいて、

暗号化された第一の暗号化鍵が添付され、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、

該第一の暗号化鍵を復号化する手段と、

復号化した該第一の暗号化鍵を用いて、情報を復号化する手段とを備え、

前記受信手段が信号を受信すると、前記復号化手段は、復号化要求の有無と復号化対象の情報とを判断し、第二の暗号化鍵に対応した第二の復号化鍵で該第一の暗号化鍵を復号化するか、あるいは、該第二の暗号化鍵に対応した第二の復号化鍵で該第一の暗号化鍵を復号化することによって復号化要求の有無を判断するセッション制御サーバ。

１８．請求項１７記載のセッション制御サーバにおいて、

前記第一の暗号化鍵をセッション単位に記憶する手段を備え、

該第一の暗号化鍵を同一セッション内で、情報の復号化に再利用するセッション制御サーバ。

１９．ネットワークを介してセッション制御サーバと通信可能に接続され、前記セッション制御サーバとの間で信号送受信を行うことによって他の通信装置とのセッションを確立する通信装置において、

暗号化された第一の暗号化鍵が添付され、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、

該第一の暗号化鍵を復号化する手段と、

得られた該第一の暗号化鍵により情報を復号化する手段と、

該第一の暗号化鍵をセッション単位に記憶する手段と、

該第一の暗号化鍵を用いて情報を暗号化する手段と、

該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、

同一セッション内の情報の暗号化および復号化に、前記第一の暗号化鍵を利用する着信側の通信装置。

２０．請求項１６記載の通信装置において、

前記第一の暗号化鍵をセッション単位に記憶する手段と、

該第一の暗号化鍵を用いて情報を暗号化する手段と、

該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段と、

該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、

該第一の暗号化鍵を用いて情報を復号化する手段とを備え、

同一セッション内の情報の暗号化および復号化に、前記第一の暗号化鍵を利用する発信側の通信装置。

２１．請求項１９記載の通信装置において、

セッション単位に管理した前記第一の暗号化鍵を周期的に更新する手段を備え、

該周期的更新手段は、新規に該第一の暗号化鍵を生成する手段と、

該第一の暗号化鍵を、任意の第二の暗号化鍵により暗号化する暗号化鍵暗号化手段と、

任意の第二の暗号化鍵で暗号化した該第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段と
を備えた通信装置。

２２．請求項２０記載の通信装置において、

セッション単位に管理した前記第一の暗号化鍵を周期的に更新する手段を備え、

該周期的更新手段は、新規に該第一の暗号化鍵を生成する手段と、

該第一の暗号化鍵を、任意の第二の暗号化鍵で暗号化する暗号化鍵暗号化手段と、

任意の第二の暗号化鍵で暗号化した該第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段と
を備えた通信装置。

２３．請求項１８記載のセッション制御サーバにおいて、

セッション単位に管理した前記第一の暗号化鍵を、周期的に更新する手段を備え、

該周期的更新手段は、任意の第二の暗号化鍵で暗号化した該第一の暗号化鍵が添付され、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段を備えたセッション制御サーバ。

２４．ネットワークを介して互いに通信可能に接続され、信号送受信を行うことによってセッションを確立する通信システムにおいて、

送信信号の守秘性を保持するために暗号化した情報を含む信号を送信する際に、暗号化のための第一の暗号化鍵を生成する手段と、該第一の暗号化鍵を用いて情報を暗号化する手段と、該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する暗号化鍵暗号化手段と、任意の第二の暗号化鍵で暗号化した第一の暗号化鍵を添付した、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、前記暗号化鍵暗号化手段は、該第一の暗号化鍵を、送信先の通信装置または１以上の該セッション制御サーバの各々が保有する第二の暗号化鍵を用いて暗号化し、前記送信手段は、暗号化された該第一の暗号化鍵と、該第一の暗号化鍵により暗号化された情報を含む信号と、該セッション制御サーバに対する復号化要求指示とを送信する第１の通信装置と、

暗号化した第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、該第一の暗号化鍵を復号化する手段と、得られた該第一の暗号化鍵により情報を復号化する手段と、該第一の暗号化鍵をセッション単位に記憶する手段と、該第一の暗号化鍵を用いて情報を暗号化する

手段と、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、同一セッション内の情報の暗号化および復号化に、前記第一の暗号化鍵を利用する第２の通信装置と、

暗号化された第一の暗号化鍵が添付され、かつ該第一の暗号化鍵で暗号化された信号を受信する手段と、該第一の暗号化鍵を復号化する手段と、復号化した該第一の暗号化鍵を用いて、情報を復号化する復号化手段とを備え、前記受信手段が信号を受信すると、前記復号化手段は、復号化要求の有無を判断し、第二の暗号化鍵に対応した第二の復号化鍵で該第一の暗号化鍵を復号化するか、あるいは、該第二の暗号化携に対応した第二の復号化鍵で該第一の暗号化鍵を復号化することによって復号化要求の有無を判断するセッション制御サーバと
を有する通信システム。

２５．ネットワークを介して互いに通信可能に接続され、信号送受信を行うことによってセッションを確立する通信システムにおいて、

暗号化された第一の暗号化鍵が添付され、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、該第一の暗号化鍵を復号化する手段と、得られた該第一の暗号化鍵により情報を復号化する手段と、該第一の暗号化鍵をセッション単位に記憶する手段と、該第一の暗号化鍵を用いて情報を暗号化する手段と、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、同一セッション内の情報の暗号化および復号化に、前記第一の暗号化鍵を利用する着信側の通信装置と、

送信信号の守秘性を保持するために暗号化した情報を送信する際に、情報暗号化のための第一の暗号化鍵を生成する手段と、該第一の暗号化鍵を用いて情報を暗号化する手段と、該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する暗号化鍵暗号化手段と、任意の第二の暗号化鍵で暗号化した第一の暗号化鍵を添付し、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段と、前記第一の暗号化鍵をセッション単位に記憶する手段と、該第一の暗号化鍵を用いて情報を暗号化する手段と、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段と、該第一の暗号化鍵で暗号化された情報を含む信号を受信する手

段と、該第一の暗号化鍵を用いて情報を復号化する手段とを備え、前記暗号化鍵暗号化手段は、該第一の暗号化鍵を、送信先の通信装置または１以上の該セッション制御サーバの各々が保有する第二の暗号化鍵を用いて暗号化し、前記送信手段は、暗号化された該第一の暗号化鍵と、該第一の暗号化鍵で暗号化された情報と、該セッション制御サーバに対する該情報の復号化要求指示とを送信し、同一セッション内の情報の暗号化および復号化に、前記第一の暗号化鍵を利用する発信側の通信装置と、

暗号化された第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、該第一の暗号化鍵を復号化する手段と、復号化した該第一の暗号化鍵を用いて、情報を復号化する手段と、前記第一の暗号化鍵をセッション単位に記憶する手段を備え、前記受信手段が信号を受信すると、前記復号化手段は、復号化要求の有無と復号化対象の情報とを判断し、第二の暗号化鍵に対応した第二の復号化鍵で該第一の暗号化鍵を復号化するか、あるいは、該第二の暗号化携に対応した第二の復号化鍵で該第一の暗号化鍵を復号化することによって復号化要求の有無を判断し、該第一の暗号化鍵を同一セッション内で、情報の復号化に再利用するセッション制御サーバと
を有することを特徴とした通信システム。

２６．ネットワークを介して互いに通信可能に接続され、信号送受信を行うことによってセッションを確立する通信システムにおいて、

暗号化した第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、該第一の暗号化鍵を復号化する手段と、得られた該第一の暗号化鍵により情報を復号化する手段と、該第一の暗号化鍵をセッション単位に記憶する手段と、該第一の暗号化鍵を用いて情報を暗号化する手段と、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段と、セッション単位に管理した前記第一の暗号化鍵を、周期的に更新する手段を備え、同一セッション内の情報の暗号化および復号化に、前記第一の暗号化鍵を利用し、該周期的更新手段は、新規に該第一の暗号化鍵を生成する手段と、該第一の暗号化鍵を、任意の第二の暗号化鍵により暗号化する暗号化鍵暗号化手段と、任意の

第二の暗号化鍵で暗号化された該第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備えた通信装置と、

暗号化された第一の暗号化鍵が添付され、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、該第一の暗号化鍵を復号化する手段と、復号化した該第一の暗号化鍵を用いて、情報を復号化する手段と、前記第一の暗号化鍵を周期的に更新する手段と、前記第一の暗号化鍵をセッション単位に記憶する手段とを備え、前記受信手段が信号を受信すると、前記復号化手段は、復号化要求の有無と復号化対象の情報とを判断し、第二の暗号化鍵に対応した第二の復号化鍵で該第一の暗号化鍵を復号化するか、あるいは、該第二の暗号化携に対応した第二の復号化鍵で該第一の暗号化鍵を復号化することによって復号化要求の有無を判断し、かつ該第一の暗号化鍵を同一セッション内で、情報の復号化に再利用するセッション制御サーバと
を有することを特徴とした通信システム。

２７．ネットワークを介して互いに通信可能に接続され、信号送受信を行うことによってセッションを確立する通信システムにおいて、

前記第一の暗号化鍵をセッション単位に記憶する手段と、該第一の暗号化鍵を用いて情報を暗号化する手段と、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段と、該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、該第一の暗号化鍵を用いて情報を復号化する手段と、セッション単位に管理した前記第一の暗号化鍵を、周期的に更新する手段を備え、該周期的更新手段は、新規に該第一の暗号化鍵を生成する手段と、該第一の暗号化鍵を、任意の第二の暗号化鍵で暗号化する暗号化鍵暗号化手段と、任意の第二の暗号化鍵で暗号化された該第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備えた通信装置と、

暗号化された第一の暗号化鍵が添付され、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、該第一の暗号化鍵を復号化する手段と、復号化した該第一の暗号化鍵を用いて、情報を復号化する手段と、前記第一の暗号化鍵を周期的に更新する手段と、前記第一の暗号化鍵をセッション単位に

記憶する手段とを備え、前記受信手段が信号を受信すると、前記復号化手段は、復号化要求の有無と復号化対象の情報とを判断し、第二の暗号化鍵に対応した第二の復号化鍵で該第一の暗号化鍵を復号化するか、あるいは、該第二の暗号化携に対応した第二の復号化鍵で該第一の暗号化鍵を復号化することによって復号化要求の有無を判断し、該第一の暗号化鍵を同一セッション内で、情報の復号化に再利用するセッション制御サーバと
を有することを特徴とした通信システム。

２８．通信装置で生成されたセッション制御信号が、信頼されるセッション制御サーバと、信頼されないセッション制御サーバとを経由して他の通信装置に送信される通信方法において、

信頼されるセッション制御サーバは、該通信装置から送信された信号を受信すると、復号化判断手段により復号化要求の有無を判断し、復号化要求があれば、暗号化鍵復号化手段により第一の暗号化鍵の復号化を行い、復号化された該第一の暗号化鍵を用いて信号復号化手段により情報を復号化し、該情報を信頼されないセッション制御サーバに送信し、該セッション制御サーバは、これを受信し、前と同一処理を施して着信側通信装置に送信し、該着信側通信装置は、受信した信号の情報が第一の暗号化鍵で暗号化されており、かつ該第一の暗号化鍵が暗号化されて添付されているときは、自身の第二の暗号化鍵に対応する第二の復号化鍵を用いて暗号化鍵復号化手段により復号化し、第一の暗号化鍵を取得し、該第一の暗号化鍵を用いて暗号化された情報を信号復号化手段により復号化する通信方法。

２９．セッション制御サーバがセッション確立中、あるいは、セッション変更中に得られた情報を基にＮＡＴ／ファイヤウォール装置のフィルタリング条件を変更する通信方法において、

セッション制御サーバは、通信装置の主情報通信径路のＩＰアドレスおよびポート番号を基に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求し、不特定ＩＰアドレスから特定ＩＰアドレスおよびポート番

号宛のパケットを通過させ、その後、他の通信装置から受信した暗号化情報を第一暗号化鍵を用いて復号化し、該通信装置の主情報通信径路のＩＰアドレスおよびポート番号を基に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求し、特定ＩＰアドレスから特定ＩＰアドレスおよびポート番号宛のパケットを通過させ、その後、通信装置からメッセージの切断信号を受信すると、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求し、指定ＩＰアドレスから指定ＩＰアドレスおよびポート番号宛のパケットを不通過とさせる通信方法。

３０．セッション制御サーバがセッション確立中、あるいは、セッション変更中に得られた情報を基に、暗号化された主情報について通信記録を可能にする通信方法において、

セッション制御サーバは、通信装置の主情報通信径路のＩＰアドレスおよびポート番号を基に、ＮＡＴ／ファイヤウォール装置に対して、フィルタリング条件変更要求に加えて、主情報転送を指示し、該ＮＡＴ／ファイヤウォール装置から主情報を受信すると、取得済みの主情報暗号化の鍵情報を用いて主情報復号化手段により復号化を行い、復号化が終了すると、復号化された主情報、あるいは、暗号化された主情報とその鍵情報とを記録する通信方法。

３１．通信装置で生成したセッション制御信号が、信頼されるセッション制御サーバと、信頼されないセッション制御サーバとを経由して他の通信装置に送信されるセッション制御用プログラムであって、

信頼されるセッション制御サーバのコンピュータに、該通信装置から送信された信号を受信する手順、復号化判断手段により復号化要求の有無を判断する手順、復号化要求があれば、暗号化鍵復号化手段により第一の暗号化鍵の復号化を行う手順、復号化された該第一の暗号化鍵を用いて信号復号化手段により情報を復号化する手順、および該情報を含む信号を信頼されないセッション制御サーバに送信する手順実行させるためのセッション制御用プログラム。

３２．セッション制御サーバがセッション確立中、あるいは、セッション変更中に得られた情報を基にＮＡＴ／ファイヤウォール装置のフィルタリング条件を変更するセッション制御用プログラムであって、

セッション制御サーバのコンピュータに、通信装置の主情報通信径路のＩＰアドレスおよびポート番号を基に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求する手順、不特定ＩＰアドレスから特定ＩＰアドレスおよびポート番号宛のパケットを通過させる手順、その後、他の通信装置から受信した暗号化情報を第一暗号化鍵を用いて復号化する手順、該通信装置の主情報通信径路のＩＰアドレスおよびポート番号を基に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求する手順、特定ＩＰアドレスから特定ＩＰアドレスおよびポート番号宛のパケットを通過させる手順、その後、通信装置からメッセージの切断信号を受信する手順、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求する手順、および指定ＩＰアドレスから指定ＩＰアドレスおよびポート番号宛のパケットを不通過とさせる手順を実行させるためのセッション制御用プログラム。

３３．セッション制御サーバがセッション確立中、あるいは、セッション変更中に得られた情報を基に、暗号化された情報について通信記録を可能にするセッション制御用プログラムであって、

セッション制御サーバのコンピュータに、通信装置の主情報通信径路のＩＰアドレスおよびポート番号を基に、ＮＡＴ／ファイヤウォール装置に対して、フィルタリング条件変更要求に加えて、主情報転送を指示する手順、該ＮＡＴ／ファイヤウォール装置から主情報を受信する手順、取得済みの主情報暗号化の鍵情報を用いて主情報復号化手段により復号化を行う手順、および復号化が終了すると、復号化された主情報、あるいは、暗号化された主情報とその鍵情報とを記録する手順実行させるためのセッション制御用プログラム。

３４．請求項３１に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

３５．請求項３２に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

３６．請求項３３に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

３７．ネットワークを介してセッション制御サーバと通信可能に接続され、１以上の該セッション制御サーバを経由して他の通信装置との間で信号の送受信を行うことによって該他の通信装置とのセッションを確立する通信装置において、

送信信号の守秘性を保つために暗号化した情報を送信する際に、暗号化のための第一の暗号化鍵を生成する手段と、

該第一の暗号化鍵を用いて情報を暗号化する手段と、

該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する手段と、

暗号化された該第一の暗号化鍵を添付して、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、

該第一の暗号化鍵を第二の暗号化鍵で暗号化する手段は、信号内情報の参照のみ、もしくは、参照と変更との両方を許容された１つのセッション制御サーバの第二の暗号化鍵により、第一の暗号化鍵を暗号化し、

該第一の暗号化鍵で暗号化された情報を送信する手段は、前記暗号化された第一の暗号化鍵と、該第一の暗号化鍵により暗号化された情報と、該セッション制御サーバに対する復号化要求指示、もしくは復号化要求指示と変更許容通知を送信する通信装置。

３８．ネットワークを介して複数の通信装置と他のセッション制御サーバと通信可能に接続され、発信側の通信装置もしくは該他のセッション制御サーバから送信された信号を受信し、受信された信号を着信側の通信装置もしくは該他のセッション制御サーバに送信することによって前記発信側の通信装置と前記着信側の通信装置とのセッションを確立させるセッション制御サーバにおいて、

暗号化された第一の暗号化鍵が添付され、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、

自らの第二の暗号化鍵に対応する第二の復号化鍵により第一の暗号化鍵を復号化する手段と、

復号化して得た第一の暗号化鍵を用いて情報を復号化する手段と、

復号化して得た第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する手段と、

任意の第二の暗号化鍵で暗号化した後、復号化して得た第一の暗号化鍵を添付して、復号化して得た第一の暗号化鍵で暗号化されている情報を含む信号を送信する手段と

を備え、

前記受信手段が暗号化された情報を含む信号を受信した際に、復号化要求の有無を判断し、該第二の暗号化鍵に対応した第二の復号化鍵で暗号化鍵を復号化するか、あるいは、該第二の暗号化鍵に対応した第二の復号化鍵で該暗号化鍵を復号化することによって復号化要求の有無を判断するか、あるいは、その両方を行うことによって該第一の暗号化鍵を取得し、

前記情報復号化手段が該第一の暗号化鍵で暗号化された情報を復号化し、

さらに、前記暗号化手段は、信号送受信時に経由し、かつ開示のみあるいは開示と変更の両方を許容された前記他のセッション制御サーバの第二の暗号化鍵、もしくは送信先の通信装置の第二の暗号化鍵により、取得された第一の暗号化鍵を暗号化し、

前記送信手段は、該暗号化された第一の暗号化鍵と、取得された第一の暗号化鍵により暗号化されている情報と、第二の暗号化鍵が該他のセッション制御サーバの暗号化鍵である場合には、該他のセッション制御サーバに対する復号化要求指示、もしくは復号化要求指示と変更許容通知を送信するセッション制御サーバ。

３９．請求項３８記載のセッション制御サーバにおいて、

前記各手段に加えて、送信信号の守秘性を保持するために暗号化した情報を含む信号を送信する際に、暗号化のための新たな第一の暗号化鍵を生成する手段と、

生成した該第一の暗号化鍵を用いて情報を暗号化する手段と、

生成した該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する手段と、

該第二の暗号化鍵で暗号化した生成した第一の暗号化鍵を添付し、かつ該生成した第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、

前記第一の暗号化鍵の暗号化手段は、信号送受信時に経由し、かつ参照のみ、もしくは、参照と変更との両方を許容された他のセッション制御サーバの第二の暗号化鍵、もしくは送信先の通信装置の第二の暗号化鍵により、該生成した第一の暗号化鍵を暗号化し、

前記送信手段は、該暗号化された生成した第一の暗号化鍵と、該生成した第一の暗号化鍵により暗号化された情報と、第二の暗号化鍵が該他のセッション制御サーバの暗号化鍵である場合には、該他のセッション制御サーバに対する復号化要求指示、もしくは復号化要求指示と変更許容通知を送信するセッション制御サーバ。

４０．請求項３８記載のセッション制御サーバにおいて、

前記第一の暗号化鍵を、セッションおよび対向装置単位に記憶する手段と、

該第一の暗号化鍵を、同一セッションで、かつ同一対向装置内の情報の暗号化および復号化の少なくともいずれかに再利用する再利用手段とを備えたセッション制御サーバ。

４１．ネットワークを介してセッション制御サーバと通信可能に接続され、前記セッション制御サーバとの間で信号の送受信を行うことによって他の通信装置とのセッションを確立する通信装置において、

暗号化した第一の暗号化鍵を添付して、暗号化された情報を含む信号を受信する手段と、

該第一の暗号化鍵を復号化する手段と、

情報を該第一の暗号化鍵で復号化する手段と、

セッションおよび対向装置単位に該第一の暗号化鍵を記憶する手段と、

該第一の暗号化鍵を用いて情報を暗号化する手段と、

該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、

該記憶する手段に記憶された第一の暗号化鍵を、同一セッション内の情報の暗号化および復号化の少なくともいずれかに利用する通信装置。

４２．請求項３７記載の通信装置において、

前記第一の暗号化鍵を、セッションと対向装置単位に記憶する手段と、

該第一の暗号化鍵を用いて情報を暗号化する手段と、

該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段と、

該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、

該第一の暗号化鍵を用いて情報を復号化する手段とを備え、

該記憶する手段に記憶された第一の暗号化鍵を、同一セッション内の情報の暗号化および復号化の少なくともいずれかに利用する通信装置。

４３．請求項３７に記載の通信装置において、

前記セッションおよび対向装置単位に管理した第一の暗号化鍵を周期的に更新する手段を備え、

該更新手段は、

新規に第一の暗号化鍵を生成する手段と、

該第一の暗号化鍵を、任意の第二の暗号化鍵、もしくは既に記憶されている第一の暗号化鍵により暗号化する暗号化鍵暗号化手段と、

任意の第二の暗号化鍵で暗号化した該第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段を備えた通信装置。

４４．請求項４１に記載の通信装置において、

前記セッションおよび対向装置単位に管理した第一の暗号化鍵を周期的に更新する手段を備え、

該更新手段は、

新規に第一の暗号化鍵を生成する手段と、

該第一の暗号化鍵を、任意の第二の暗号化鍵、もしくは既に記憶されている第一の暗号化鍵により暗号化する暗号化鍵暗号化手段と、

任意の第二の暗号化鍵で暗号化した該第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段を備えた通信装置。

４５．請求項３７に記載のセッション制御サーバにおいて、

前記セッションと対向装置単位に管理した第一の暗号化鍵を周期的に更新する手段と、

任意の第二の暗号化鍵、もしくは既に記憶されている第一の暗号化鍵により暗号化された、新たな第一の暗号化鍵を添付し、該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、

更新した新たな第一の暗号化鍵を用いて、情報を暗号化する手段と、

更新された新たな暗号化鍵を，暗号化された情報とともに送信する手段とを備え、

該送信手段は、前記任意の第二の暗号化鍵、もしくは前記既に記憶されている第一の暗号化鍵で暗号化された、新たな第一の暗号化鍵を添付し、該第一の暗号化鍵で暗号化された情報を送信するセッション制御サーバ。

４６．請求項３８に記載のセッション制御サーバにおいて、

前記セッションと対向装置単位に管理した第一の暗号化鍵を周期的に更新する手段と、

任意の第二の暗号化鍵、もしくは既に記憶されている第一の暗号化鍵により暗号化された、新たな第一の暗号化鍵を添付し、該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、

更新した新たな第一の暗号化鍵を用いて、情報を暗号化する手段と、

更新された新たな暗号化鍵を，暗号化された情報とともに送信する手段とを備え、

該送信手段は、前記任意の第二の暗号化鍵、もしくは前記既に記憶されている第一の暗号化鍵で暗号化された、新たな第一の暗号化鍵を添付し、該第一の暗号化鍵で暗号化された情報を含む信号を送信するセッション制御サーバ。

４７．ネットワークを介して互いに通信可能に接続され、通信装置相互間で信号の送受信を行うことによってセッションを確立する通信システムにおいて、

暗号化した第一の暗号化鍵を添付して、該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段、自らの第二の暗号化鍵に対応する第二の復号化鍵により第一の暗号化鍵を復号化する手段、復号化して得た第一の暗号化鍵を用いて情報を復号化する手段、復号化して得た第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する手段、ならびに任意の第二の暗号化鍵で暗号化した後、復号化して得た第一の暗号化鍵を添付して、復号化して得た第一の暗号化鍵で暗号化されている情報を含む信号を送信する手段を備え、前記受信手段が暗号化された情報を受信した際に、復号化要求の有無を判断し、該第二の暗号化鍵に対応した第二の復号化鍵で暗号化鍵を復号化するか、あるいは、該第二の暗号化鍵に対応した第二の復号化鍵で該暗号化鍵を復号化することによって復号化要求の有無を判断するか、あるいは、その両方を行うことによって該第一の暗号化鍵を取得し、前記情報復号化手段が該第一の暗号化鍵で暗号化された情報を復号化し、さらに、前記暗号化手段は、信号送受信時に経由し、かつ開示のみあるいは開示と変更の両方を許容された前記他のセッション制御サーバの第二の暗号化鍵、もしくは送信先の通信装置の第二の暗号化鍵により、取得された第一の暗号化鍵を暗号化し、前記送信手段は、該暗号化された第一の暗号化鍵と、取得された第一の暗号化鍵により暗号化されている情報と、第二の暗号化鍵が該他のセッション制御サーバの暗号化鍵である場合には、該他のセッション制御サーバに対する復号化要求指示を送信するセッション制御サーバと、

送信信号の守秘性を保つために暗号化した情報を含む信号を送信する際に、暗号化のための第一の暗号化鍵を生成する手段、該第一の暗号化鍵を用いて情報を暗号化する手段、該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する手段、ならびに暗号化された該第一の暗号化鍵を添付して、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段を備え、該第一の暗号化鍵を第二の暗号化鍵で暗号化する手段は、開示のみもしくは開示と変更の両方を許容された１つのセッション制御サーバの第二の暗号化鍵、もしくは送信先の通信装置の第二の暗号化鍵により、第一の暗号化鍵を暗号化し、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段は、前記暗号化された第一の暗号化鍵と、該第一の暗号化鍵により暗号化された情報と、該第二の暗号化鍵が前記セッション制御サーバの暗号化鍵である場合には、該セッション制御サーバに対する復号化要求指示を送信する通信装置、あるいは、

前記各手段に加えて、送信信号の守秘性を保持するために暗号化した情報を含む信号を送信する際に、暗号化のための新たな第一の暗号化鍵を生成する手段、生成した該第一の暗号化鍵を用いて情報を暗号化する手段、生成した該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する手段、該第二の暗号化鍵で暗号化した生成した第一の暗号化鍵を添付し、かつ該生成した第一の暗号化鍵で暗号化された情報を含む信号を送信する手段を備え、前記第一の暗号化鍵の暗号化手段は、信号送受信時に経由し、かつ参照のみ、もしくは、参照と変更の両方を許容された他のセッション制御サーバの第二の暗号化鍵、もしくは送信先の通信装置の第二の暗号化鍵により、該生成した第一の暗号化鍵を暗号化し、前記送信手段は、該暗号化された生成した第一の暗号化鍵と、該生成した第一の暗号化鍵により暗号化された情報と、第二の暗号化鍵が該他のセッション制御サーバの暗号化鍵である場合には、該他のセッション制御サーバに対する復号化要求指示を送信する通信装置と、

暗号化された第一の暗号化鍵が添付され、かつ暗号化された情報を含む信号を受信する手段と、

該第一の暗号化鍵を復号化する手段、情報を該第一の暗号化鍵で復号化する手段、セッションと対向装置単位に該第一の暗号化鍵を記憶する手段、該第

一の暗号化鍵を用いて情報を暗号化する手段、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段を備え、該記憶する手段に記憶された第一の暗号化鍵を、同一セッション内の情報の暗号化および復号化の少なくともいずれかに利用する着信側通信装置と、

前記第一の暗号化鍵を、セッションと対向装置単位に記憶する手段、該第一の暗号化鍵を用いて情報を暗号化する手段、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段、該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段、ならびに該第一の暗号化鍵を用いて情報を復号化する手段を備え、該記憶する手段に記憶された第一の暗号化鍵を、同一セッション内の情報の暗号化および復号化の少なくともいずれかに利用する発信側通信装置とを有する通信システム。

４８．請求項４７記載の通信システムにおいて、

前記第一の暗号化鍵を、セッションと対向装置単位に記憶する手段、該第一の暗号化鍵を、同一セッションで、かつ同一対向装置内の情報の暗号化および復号化の少なくともいずれかに再利用する再利用手段を備えたセッション制御サーバと、

暗号化した第一の暗号化鍵を添付して、暗号化された情報を含む信号を受信する手段、第一の暗号化鍵を復号化する手段、情報を該第一の暗号化鍵で復号化する手段、セッションと対向装置単位に該第一の暗号化鍵を記憶する手段、該第一の暗号化鍵を用いて情報を暗号化する手段、ならびに該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段を備え、該記憶する手段に記憶された第一の暗号化鍵を、同一セッション内の情報の暗号化および復号化の少なくともいずれかに利用する着信側通信装置と、

前記第一の暗号化鍵を、セッションと対向装置単位に記憶する手段、該第一の暗号化鍵を用いて情報を暗号化する手段、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段、該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段、ならびに該第一の暗号化鍵を用いて情報を復号化する手段

を備え、該記憶する手段に記憶された第一の暗号化鍵を、同一セッション内の情報の暗号化および復号化の少なくともいずれかに利用する発信側通信装置と
を有する通信システム。

４９．請求項４７記載の通信システムにおいて、

前記セッションと対向装置単位に管理した第一の暗号化鍵を周期的に更新する手段、任意の第二の暗号化鍵、もしくは既に記憶されている第一の暗号化鍵により暗号化された、新たな第一の暗号化鍵を添付し、該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段、更新した新たな第一の暗号化鍵を用いて、情報を暗号化する手段、ならびに暗号化された情報とともに更新された新たな暗号化鍵を送信する手段を備え、前記送信手段は、任意の第二の暗号化鍵、もしくは前記既に記憶されている第一の暗号化鍵により暗号化された、新たな第一の暗号化鍵を添付し、該第一の暗号化鍵で暗号化された情報を含む信号を送信するセッション制御サーバと、

前記第一の暗号化鍵を、セッションと対向装置単位に記憶する手段、該第一の暗号化鍵を用いて情報を暗号化する手段、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段、該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段、ならびに該第一の暗号化鍵を用いて情報を復号化する手段を備え、該記憶する手段に記憶された第一の暗号化鍵を、同一セッション内の情報の暗号化および復号化の少なくともいずれかに利用する発信側通信装置と、

前記セッションと対向装置単位に管理した第一の暗号化鍵を周期的に更新する手段を備え、該更新手段は、新規に第一の暗号化鍵を生成する手段、該第一の暗号化鍵を、任意の第二の暗号化鍵により暗号化する暗号化鍵暗号化手段、ならびに任意の第二の暗号化鍵で暗号化した該第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段を備えた発信側または着信側通信装置と
を有する通信システム。

５０．発信側通信装置で生成したセッション制御信号を、信頼されるセッション制御サーバと、信頼されないセッション制御サーバとを経由して着信側通信装置に送信する通信方法において、

該発信側通信装置は、暗号化に使用した第一の暗号化鍵を、セッション制御サーバの公開された第二の暗号化鍵で暗号化し、

該セッション制御サーバに復号化要求を示す値と、復号化すべきコンテンツＩＤとを含めて送信し、

該セッション制御サーバは、復号化要求パラメータの値によって復号化要求を判断するか、暗号化された第一の暗号化鍵が設定されたデータの復号化の可否によって復号化要求を判断し、

復号化要求が有る場合には、第二の暗号化鍵に対応した第二の復号化鍵で復号化して、通信装置間制御情報の参照あるいは変更を可能とし、

通信装置間制御情報を変更した後、該第一の暗号化鍵をそのまま利用するか、あるいは新規に生成した第一の暗号化鍵を用いて、変更後の情報を暗号化し、

次のセッション制御サーバあるいは着信側通信装置に送信することを特徴する通信方法。

５１．セッション制御サーバが、セッション確立中に得られた情報を基に、ＮＡＴ／ファイヤウォール装置のフィルタリング条件を変更する通信方法において、

セッション制御サーバは、復号化する復号化鍵を判断した後、第一の暗号化鍵の復号化を行い、暗号化情報を該第一の暗号化鍵で復号化して通信装置間の制御情報を参照あるいは変更可能とし、

該制御情報を基に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求し、

その後、着信側通信装置から受信した通信装置間の制御情報を復号化して通信装置間の制御情報を参照あるいは変更可能とし、

該制御情報を基に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求し、ＮＡＴ／ファイヤウォール装置において通信装置相互間の主情報についてパケット通過を行わせる通信方法。

５２．セッション制御サーバが、セッション確立中に得られた情報を基に、暗号化された主情報について通信記録を可能にする通信方法において、

セッション制御サーバは、ＮＡＴ／ファイヤウォール装置等に対してフィルタリング条件の変更要求に加え、主情報転送を指示し、ＮＡＴ／ファイヤウォール装置等から主情報を受信すると、該主情報が暗号化されている場合には、信号送受の際、第一の暗号化鍵の復号化を行い、暗号化情報を該第一の暗号化鍵で復号化して得た通信装置間の制御情報とともに、既に取得済みの主情報暗号化の鍵を用いて復号化し、該主情報を通信記録手段に記録する通信方法。

５３．発信側通信装置で生成したセッション制御信号を、信頼されるセッション制御サーバと、信頼されないセッション制御サーバとを経由して着信側通信装置に送信する通信用プログラムであって、

該セッション制御サーバのコンピュータに、復号化要求パラメータの値によって復号化要求を判断するか、暗号化された第一の暗号化鍵が設定されたデータの復号化の可否によって復号化要求を判断する手順、復号化要求が有る場合には、第二の暗号化鍵に対応した第二の復号化鍵で復号化して、通信装置間制御情報の参照あるいは変更を可能とする手順、該第一の暗号化鍵をそのまま利用するか、あるいは新規に生成した第一の暗号化鍵を用いて、変更後の情報を暗号化する手順、および次のセッション制御サーバあるいは着信側通信装置に送信する手順を実行させるための通信用プログラム。

５４．セッション制御サーバが、セッション確立中に得られた情報を基に、ＮＡＴ／ファイヤウォール装置のフィルタリング条件を変更する通信用プログラムであって、

該セッション制御サーバのコンピュータに、復号化する復号化鍵を判断する手順、第一の暗号化鍵の復号化を行う手順、暗号化情報を該第一の暗号化鍵で復号化して通信装置間の制御情報を参照あるいは変更可能にする手順、該制御情報を基に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求する手順、着信側通信装置から受信した通信装置間の制御情報を復号化して通信装置間の制御情報を参照あるいは変更可能とする手順、および該制御情報を基に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求する手順を実行させるための通信用プログラム。

５５．セッション制御サーバが、セッション確立中に得られた情報を基に、暗号化された主情報について通信記録を行う通信用プログラムであって、

該セッション制御サーバのコンピュータに、ＮＡＴ／ファイヤウォール装置等に対してフィルタリング条件の変更要求に加え、主情報転送を指示する手順、ＮＡＴ／ファイヤウォール装置等から主情報を受信する手順、該主情報が暗号化されている場合には、信号送受の際、第一の暗号化鍵の復号化を行い、暗号化情報を該第一の暗号化鍵で復号化して得た通信装置間の制御情報とともに、既に取得済みの主情報暗号化の鍵を用いて復号化する手順、および該主情報を通信記録手段に記録する手順を実行させるための通信用プログラム。

５６．請求項５３に記載の通信用プログラムを記録したコンピュータ読み取り可能な記録媒体。

５７．請求項５４に記載の通信用プログラムを記録したコンピュータ読み取り可能な記録媒体。

５８．請求項５５に記載の通信用プログラムを記録したコンピュータ読み取り可能な記録媒体。

補正書の請求の範囲

［２００５年１月０６日（０６．０１．２００５）国際事務局受理 ：出願当初の請求の範囲１６－３６は取り下げられた；他の請求の範囲は変更なし。（１５頁)］

および前記通信装置に対して位置情報と証明書発行完了通知の信号を送信する手順を実行させるための通信用プログラム。

１３．ネットワークを介して通信可能に接続され、通信装置相互間でセッションを確立するための通信用プログラムであって、

セッション制御サーバのコンピュータに、通信装置から証明書問合せ要求信号を受信する手順、セッション制御を行う手順、自ドメイン宛てか否かを判定する手順、自ドメイン宛てであれば、信号種別を判定する手順、証明書問合せ要求であれば、証明書があるか否かを判定する手順、証明書があれば、該当する証明書を検索する手順、検索された証明書の有効性を確認する手順、前記通信装置に対して証明書通知を送信する手順、および自ドメイン宛てでない場合には、宛先のセッション制御サーバに該証明書問合せ要求信号を転送する手順を実行させるための通信用プログラム。

１４．請求項１２に記載の通信用プログラムを記録したコンピュータ読み取り可能な記録媒体。

１５．請求項１３に記載の通信用プログラムを記録したコンピュータ読み取り可能な記録媒体。

１６．（削除）

１７．（削除）

１８．（削除）

１９．（削除）

２０．（削除）

２１．（削除）

２２．（削除）

２３．（削除）

２４．（削除）

２５．（削除）

２６．（削除）

２７．（削除）

２８．（削除）

２９．（削除）

３０．（削除）

３１．（削除）

３２．（削除）

３３．（削除）

３４．（削除）

３５．（削除）

３６．（削除）

３７．ネットワークを介してセッション制御サーバと通信可能に接続され、１以上の該セッション制御サーバを経由して他の通信装置との間で信号の送受信を行うことによって該他の通信装置とのセッションを確立する通信装置において、

送信信号の守秘性を保つために暗号化した情報を送信する際に、暗号化のための第一の暗号化鍵を生成する手段と、

該第一の暗号化鍵を用いて情報を暗号化する手段と、

該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する手段と、

暗号化された該第一の暗号化鍵を添付して、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、

該第一の暗号化鍵を第二の暗号化鍵で暗号化する手段は、信号内情報の参照のみ、もしくは、参照と変更との両方を許容された１つのセッション制御サーバの第二の暗号化鍵により、第一の暗号化鍵を暗号化し、

該第一の暗号化鍵で暗号化された情報を送信する手段は、前記暗号化された第一の暗号化鍵と、該第一の暗号化鍵により暗号化された情報と、該セッション制御サーバに対する復号化要求指示、もしくは復号化要求指示と変更許容通知を送信する通信装置。

３８．ネットワークを介して複数の通信装置と他のセッション制御サーバと通信可能に接続され、発信側の通信装置もしくは該他のセッション制御サーバから送信された信号を受信し、受信された信号を着信側の通信装置もしくは該他のセッ

ション制御サーバに送信することによって前記発信側の通信装置と前記着信側の通信装置とのセッションを確立させるセッション制御サーバにおいて、

暗号化された第一の暗号化鍵が添付され、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、

自らの第二の暗号化鍵に対応する第二の復号化鍵により第一の暗号化鍵を復号化する手段と、

復号化して得た第一の暗号化鍵を用いて情報を復号化する手段と、

復号化して得た第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する手段と、

任意の第二の暗号化鍵で暗号化した後、復号化して得た第一の暗号化鍵を添付して、復号化して得た第一の暗号化鍵で暗号化されている情報を含む信号を送信する手段と

を備え、

前記受信手段が暗号化された情報を含む信号を受信した際に、復号化要求の有無を判断し、該第二の暗号化鍵に対応した第二の復号化鍵で暗号化鍵を復号化するか、あるいは、該第二の暗号化鍵に対応した第二の復号化鍵で該暗号化鍵を復号化することによって復号化要求の有無を判断するか、あるいは、その両方を行うことによって該第一の暗号化鍵を取得し、

前記情報復号化手段が該第一の暗号化鍵で暗号化された情報を復号化し、

さらに、前記暗号化手段は、信号送受信時に経由し、かつ開示のみあるいは開示と変更の両方を許容された前記他のセッション制御サーバの第二の暗号化鍵、もしくは送信先の通信装置の第二の暗号化鍵により、取得された第一の暗号化鍵を暗号化し、

前記送信手段は、該暗号化された第一の暗号化鍵と、取得された第一の暗号化鍵により暗号化されている情報と、第二の暗号化鍵が該他のセッション制御サーバの暗号化鍵である場合には、該他のセッション制御サーバに対する復

号化要求指示、もしくは復号化要求指示と変更許容通知を送信するセッション制御サーバ。

３９．請求項３８記載のセッション制御サーバにおいて、

前記各手段に加えて、送信信号の守秘性を保持するために暗号化した情報を含む信号を送信する際に、暗号化のための新たな第一の暗号化鍵を生成する手段と、

生成した該第一の暗号化鍵を用いて情報を暗号化する手段と、

生成した該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する手段と、

該第二の暗号化鍵で暗号化した生成した第一の暗号化鍵を添付し、かつ該生成した第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、

前記第一の暗号化鍵の暗号化手段は、信号送受信時に経由し、かつ参照のみ、もしくは、参照と変更との両方を許容された他のセッション制御サーバの第二の暗号化鍵、もしくは送信先の通信装置の第二の暗号化鍵により、該生成した第一の暗号化鍵を暗号化し、

前記送信手段は、該暗号化された生成した第一の暗号化鍵と、該生成した第一の暗号化鍵により暗号化された情報と、第二の暗号化鍵が該他のセッション制御サーバの暗号化鍵である場合には、該他のセッション制御サーバに対する復号化要求指示、もしくは復号化要求指示と変更許容通知を送信するセッション制御サーバ。

４０．請求項３８記載のセッション制御サーバにおいて、

前記第一の暗号化鍵を、セッションおよび対向装置単位に記憶する手段と、

該第一の暗号化鍵を、同一セッションで、かつ同一対向装置内の情報の暗号化および復号化の少なくともいずれかに再利用する再利用手段とを備えたセッション制御サーバ。

４１．ネットワークを介してセッション制御サーバと通信可能に接続され、前記セッション制御サーバとの間で信号の送受信を行うことによって他の通信装置とのセッションを確立する通信装置において、

暗号化した第一の暗号化鍵を添付して、暗号化された情報を含む信号を受信する手段と、

該第一の暗号化鍵を復号化する手段と、

情報を該第一の暗号化鍵で復号化する手段と、

セッションおよび対向装置単位に該第一の暗号化鍵を記憶する手段と、

該第一の暗号化鍵を用いて情報を暗号化する手段と、

該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、

該記憶する手段に記憶された第一の暗号化鍵を、同一セッション内の情報の暗号化および復号化の少なくともいずれかに利用する通信装置。

４２．請求項３７記載の通信装置において、

前記第一の暗号化鍵を、セッションと対向装置単位に記憶する手段と、

該第一の暗号化鍵を用いて情報を暗号化する手段と、

該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段と、

該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、

該第一の暗号化鍵を用いて情報を復号化する手段とを備え、

該記憶する手段に記憶された第一の暗号化鍵を、同一セッション内の情報の暗号化および復号化の少なくともいずれかに利用する通信装置。

４３．請求項３７に記載の通信装置において、

前記セッションおよび対向装置単位に管理した第一の暗号化鍵を周期的に更新する手段を備え、

該更新手段は、

新規に第一の暗号化鍵を生成する手段と、

該第一の暗号化鍵を、任意の第二の暗号化鍵、もしくは既に記憶されている第一の暗号化鍵により暗号化する暗号化鍵暗号化手段と、

任意の第二の暗号化鍵で暗号化した該第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段を備えた通信装置。

４４．請求項４１に記載の通信装置において、

前記セッションおよび対向装置単位に管理した第一の暗号化鍵を周期的に更新する手段を備え、

該更新手段は、

新規に第一の暗号化鍵を生成する手段と、

該第一の暗号化鍵を、任意の第二の暗号化鍵、もしくは既に記憶されている第一の暗号化鍵により暗号化する暗号化鍵暗号化手段と、

任意の第二の暗号化鍵で暗号化した該第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段を備えた通信装置。

４５．請求項３７に記載のセッション制御サーバにおいて、

前記セッションと対向装置単位に管理した第一の暗号化鍵を周期的に更新する手段と、

任意の第二の暗号化鍵、もしくは既に記憶されている第一の暗号化鍵により暗号化された、新たな第一の暗号化鍵を添付し、該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、

更新した新たな第一の暗号化鍵を用いて、情報を暗号化する手段と、

更新された新たな暗号化鍵を，暗号化された情報とともに送信する手段とを備え、

該送信手段は、前記任意の第二の暗号化鍵、もしくは前記既に記憶されている第一の暗号化鍵で暗号化された、新たな第一の暗号化鍵を添付し、該第一の暗号化鍵で暗号化された情報を送信するセッション制御サーバ。

４６．請求項３８に記載のセッション制御サーバにおいて、

前記セッションと対向装置単位に管理した第一の暗号化鍵を周期的に更新する手段と、

任意の第二の暗号化鍵、もしくは既に記憶されている第一の暗号化鍵により暗号化された、新たな第一の暗号化鍵を添付し、該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、

更新した新たな第一の暗号化鍵を用いて、情報を暗号化する手段と、

更新された新たな暗号化鍵を，暗号化された情報とともに送信する手段とを備え、

該送信手段は、前記任意の第二の暗号化鍵、もしくは前記既に記憶されている第一の暗号化鍵で暗号化された、新たな第一の暗号化鍵を添付し、該第一の暗号化鍵で暗号化された情報を含む信号を送信するセッション制御サーバ。

４７．ネットワークを介して互いに通信可能に接続され、通信装置相互間で信号の送受信を行うことによってセッションを確立する通信システムにおいて、

暗号化した第一の暗号化鍵を添付して、該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段、自らの第二の暗号化鍵に対応する第二の復号化鍵により第一の暗号化鍵を復号化する手段、復号化して得た第一の暗号化鍵を用いて情報を復号化する手段、復号化して得た第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する手段、ならびに任意の第二の暗号化鍵で暗号化した後、復

号化して得た第一の暗号化鍵を添付して、復号化して得た第一の暗号化鍵で暗号化されている情報を含む信号を送信する手段を備え、前記受信手段が暗号化された情報を受信した際に、復号化要求の有無を判断し、該第二の暗号化鍵に対応した第二の復号化鍵で暗号化鍵を復号化するか、あるいは、該第二の暗号化鍵に対応した第二の復号化鍵で該暗号化鍵を復号化することによって復号化要求の有無を判断するか、あるいは、その両方を行うことによって該第一の暗号化鍵を取得し、前記情報復号化手段が該第一の暗号化鍵で暗号化された情報を復号化し、さらに、前記暗号化手段は、信号送受信時に経由し、かつ開示のみあるいは開示と変更の両方を許容された前記他のセッション制御サーバの第二の暗号化鍵、もしくは送信先の通信装置の第二の暗号化鍵により、取得された第一の暗号化鍵を暗号化し、前記送信手段は、該暗号化された第一の暗号化鍵と、取得された第一の暗号化鍵により暗号化されている情報と、第二の暗号化鍵が該他のセッション制御サーバの暗号化鍵である場合には、該他のセッション制御サーバに対する復号化要求指示を送信するセッション制御サーバと、

送信信号の守秘性を保つために暗号化した情報を含む信号を送信する際に、暗号化のための第一の暗号化鍵を生成する手段、該第一の暗号化鍵を用いて情報を暗号化する手段、該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する手段、ならびに暗号化された該第一の暗号化鍵を添付して、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段を備え、該第一の暗号化鍵を第二の暗号化鍵で暗号化する手段は、開示のみもしくは開示と変更の両方を許容された１つのセッション制御サーバの第二の暗号化鍵、もしくは送信先の通信装置の第二の暗号化鍵により、第一の暗号化鍵を暗号化し、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段は、前記暗号化された第一の暗号化鍵と、該第一の暗号化鍵により暗号化された情報と、該第二の暗号化鍵が前記セッション制御サーバの暗号化鍵である場合には、該セッション制御サーバに対する復号化要求指示を送信する通信装置、あるいは、

前記各手段に加えて、送信信号の守秘性を保持するために暗号化した情報を含む信号を送信する際に、暗号化のための新たな第一の暗号化鍵を生成する手段、生成した該第一の暗号化鍵を用いて情報を暗号化する手段、生成した該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する手段、該第二の暗号化鍵で暗号化した生成した第一の暗号化鍵を添付し、かつ該生成した第一の暗号化鍵で暗号化された情報を含む信号を送信する手段を備え、前記第一の暗号化鍵の暗号化手段は、信号送受信時に経由し、かつ参照のみ、もしくは、参照と変更の両方を許容された他のセッション制御サーバの第二の暗号化鍵、もしくは送信先の通信装置の第二の暗号化鍵により、該生成した第一の暗号化鍵を暗号化し、前記送信手段は、該暗号化された生成した第一の暗号化鍵と、該生成した第一の暗号化鍵により暗号化された情報と、第二の暗号化鍵が該他のセッション制御サーバの暗号化鍵である場合には、該他のセッション制御サーバに対する復号化要求指示を送信する通信装置と、

暗号化された第一の暗号化鍵が添付され、かつ暗号化された情報を含む信号を受信する手段と、

該第一の暗号化鍵を復号化する手段、情報を該第一の暗号化鍵で復号化する手段、セッションと対向装置単位に該第一の暗号化鍵を記憶する手段、該第一の暗号化鍵を用いて情報を暗号化する手段、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段を備え、該記憶する手段に記憶された第一の暗号化鍵を、同一セッション内の情報の暗号化および復号化の少なくともいずれかに利用する着信側通信装置と、

前記第一の暗号化鍵を、セッションと対向装置単位に記憶する手段、該第一の暗号化鍵を用いて情報を暗号化する手段、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段、該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段、ならびに該第一の暗号化鍵を用いて情報を復号化する手段を備え、該記憶する手段に記憶された第一の暗号化鍵を、同一セッション内の

情報の暗号化および復号化の少なくともいずれかに利用する発信側通信装置とを有する通信システム。

４８．請求項４７記載の通信システムにおいて、

前記第一の暗号化鍵を、セッションと対向装置単位に記憶する手段、該第一の暗号化鍵を、同一セッションで、かつ同一対向装置内の情報の暗号化および復号化の少なくともいずれかに再利用する再利用手段を備えたセッション制御サーバと、

暗号化した第一の暗号化鍵を添付して、暗号化された情報を含む信号を受信する手段、第一の暗号化鍵を復号化する手段、情報を該第一の暗号化鍵で復号化する手段、セッションと対向装置単位に該第一の暗号化鍵を記憶する手段、該第一の暗号化鍵を用いて情報を暗号化する手段、ならびに該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段を備え、該記憶する手段に記憶された第一の暗号化鍵を、同一セッション内の情報の暗号化および復号化の少なくともいずれかに利用する着信側通信装置と、

前記第一の暗号化鍵を、セッションと対向装置単位に記憶する手段、該第一の暗号化鍵を用いて情報を暗号化する手段、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段、該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段、ならびに該第一の暗号化鍵を用いて情報を復号化する手段を備え、該記憶する手段に記憶された第一の暗号化鍵を、同一セッション内の情報の暗号化および復号化の少なくともいずれかに利用する発信側通信装置とを有する通信システム。

４９．請求項４７記載の通信システムにおいて、

前記セッションと対向装置単位に管理した第一の暗号化鍵を周期的に更新する手段、任意の第二の暗号化鍵、もしくは既に記憶されている第一の暗号化鍵により暗号化された、新たな第一の暗号化鍵を添付し、該第一の暗号化鍵で

暗号化された情報を含む信号を受信する手段、更新した新たな第一の暗号化鍵を用いて、情報を暗号化する手段、ならびに暗号化された情報とともに更新された新たな暗号化鍵を送信する手段を備え、前記送信手段は、任意の第二の暗号化鍵、もしくは前記既に記憶されている第一の暗号化鍵により暗号化された、新たな第一の暗号化鍵を添付し、該第一の暗号化鍵で暗号化された情報を含む信号を送信するセッション制御サーバと、

前記第一の暗号化鍵を、セッションと対向装置単位に記憶する手段、該第一の暗号化鍵を用いて情報を暗号化する手段、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段、該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段、ならびに該第一の暗号化鍵を用いて情報を復号化する手段を備え、該記憶する手段に記憶された第一の暗号化鍵を、同一セッション内の情報の暗号化および復号化の少なくともいずれかに利用する発信側通信装置と、

前記セッションと対向装置単位に管理した第一の暗号化鍵を周期的に更新する手段を備え、該更新手段は、新規に第一の暗号化鍵を生成する手段、該第一の暗号化鍵を、任意の第二の暗号化鍵により暗号化する暗号化鍵暗号化手段、ならびに任意の第二の暗号化鍵で暗号化した該第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段を備えた発信側または着信側通信装置と

を有する通信システム。

５０．発信側通信装置で生成したセッション制御信号を、信頼されるセッション制御サーバと、信頼されないセッション制御サーバとを経由して着信側通信装置に送信する通信方法において、

該発信側通信装置は、暗号化に使用した第一の暗号化鍵を、セッション制御サーバの公開された第二の暗号化鍵で暗号化し、

該セッション制御サーバに復号化要求を示す値と、復号化すべきコンテンツＩＤとを含めて送信し、

該セッション制御サーバは、復号化要求パラメータの値によって復号化要求を判断するか、暗号化された第一の暗号化鍵が設定されたデータの復号化の可否によって復号化要求を判断し、

復号化要求が有る場合には、第二の暗号化鍵に対応した第二の復号化鍵で復号化して、通信装置間制御情報の参照あるいは変更を可能とし、

通信装置間制御情報を変更した後、該第一の暗号化鍵をそのまま利用するか、あるいは新規に生成した第一の暗号化鍵を用いて、変更後の情報を暗号化し、

次のセッション制御サーバあるいは着信側通信装置に送信することを特徴する通信方法。

５１．セッション制御サーバが、セッション確立中に得られた情報を基に、ＮＡＴ／ファイヤウォール装置のフィルタリング条件を変更する通信方法において、

セッション制御サーバは、復号化する復号化鍵を判断した後、第一の暗号化鍵の復号化を行い、暗号化情報を該第一の暗号化鍵で復号化して通信装置間の制御情報を参照あるいは変更可能とし、

該制御情報を基に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求し、

その後、着信側通信装置から受信した通信装置間の制御情報を復号化して通信装置間の制御情報を参照あるいは変更可能とし、

該制御情報を基に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求し、ＮＡＴ／ファイヤウォール装置において通信装置相互間の主情報についてパケット通過を行わせる通信方法。

５２．セッション制御サーバが、セッション確立中に得られた情報を基に、暗号化された主情報について通信記録を可能にする通信方法において、

セッション制御サーバは、ＮＡＴ／ファイヤウォール装置等に対してフィルタリング条件の変更要求に加え、主情報転送を指示し、ＮＡＴ／ファイヤウォール装置等から主情報を受信すると、該主情報が暗号化されている場合には、信号送受の際、第一の暗号化鍵の復号化を行い、暗号化情報を該第一の暗号化鍵で復号化して得た通信装置間の制御情報とともに、既に取得済みの主情報暗号化の鍵を用いて復号化し、該主情報を通信記録手段に記録する通信方法。

５３．発信側通信装置で生成したセッション制御信号を、信頼されるセッション制御サーバと、信頼されないセッション制御サーバとを経由して着信側通信装置に送信する通信用プログラムであって、

該セッション制御サーバのコンピュータに、復号化要求パラメータの値によって復号化要求を判断するか、暗号化された第一の暗号化鍵が設定されたデータの復号化の可否によって復号化要求を判断する手順、復号化要求が有る場合には、第二の暗号化鍵に対応した第二の復号化鍵で復号化して、通信装置間制御情報の参照あるいは変更を可能とする手順、該第一の暗号化鍵をそのまま利用するか、あるいは新規に生成した第一の暗号化鍵を用いて、変更後の情報を暗号化する手順、および次のセッション制御サーバあるいは着信側通信装置に送信する手順を実行させるための通信用プログラム。

５４．セッション制御サーバが、セッション確立中に得られた情報を基に、ＮＡＴ／ファイヤウォール装置のフィルタリング条件を変更する通信用プログラムであって、

該セッション制御サーバのコンピュータに、復号化する復号化鍵を判断する手順、第一の暗号化鍵の復号化を行う手順、暗号化情報を該第一の暗号化鍵で復号化して通信装置間の制御情報を参照あるいは変更可能にする手順、該制御情報を基に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求する手順、着信側通信装置から受信した通信装置間の制御情報を復号化

して通信装置間の制御情報を参照あるいは変更可能とする手順、および該制御情報を基に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求する手順を実行させるための通信用プログラム。

５５．セッション制御サーバが、セッション確立中に得られた情報を基に、暗号化された主情報について通信記録を行う通信用プログラムであって、

該セッション制御サーバのコンピュータに、ＮＡＴ／ファイヤウォール装置等に対してフィルタリング条件の変更要求に加え、主情報転送を指示する手順、ＮＡＴ／ファイヤウォール装置等から主情報を受信する手順、該主情報が暗号化されている場合には、信号送受の際、第一の暗号化鍵の復号化を行い、暗号化情報を該第一の暗号化鍵で復号化して得た通信装置間の制御情報とともに、既に取得済みの主情報暗号化の鍵を用いて復号化する手順、および該主情報を通信記録手段に記録する手順を実行させるための通信用プログラム。

５６．請求項５３に記載の通信用プログラムを記録したコンピュータ読み取り可能な記録媒体。

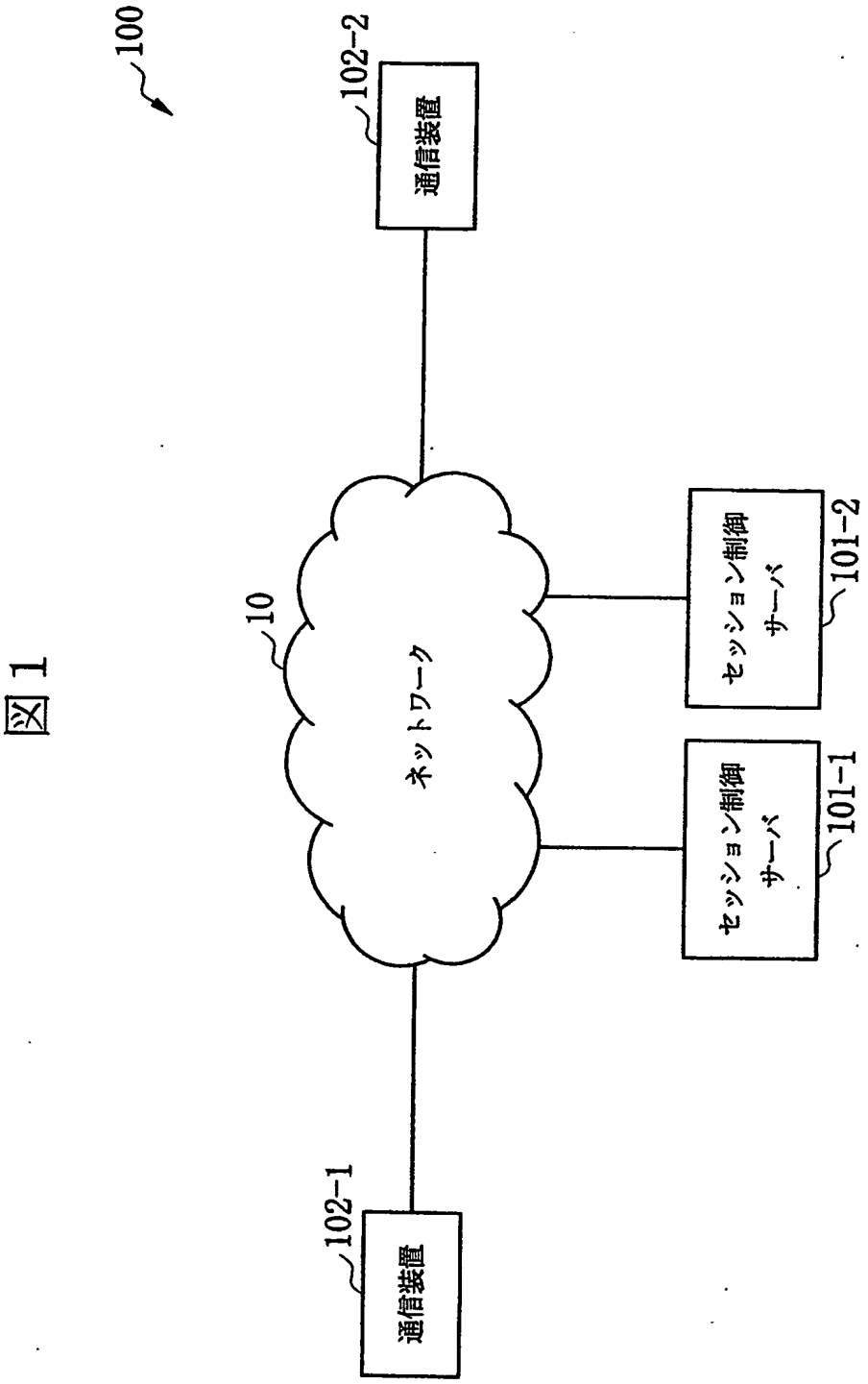
５７．請求項５４に記載の通信用プログラムを記録したコンピュータ読み取り可能な記録媒体。

５８．請求項５５に記載の通信用プログラムを記録したコンピュータ読み取り可能な記録媒体。

条約第１９条（１）に基づく説明書

補正前の請求項１６～３６を削除しました。

図1


100
102-2
通信装置
10
ネットワーク
セッション制御サーバ
101-2
セッション制御サーバ
101-1
102-1
通信装置

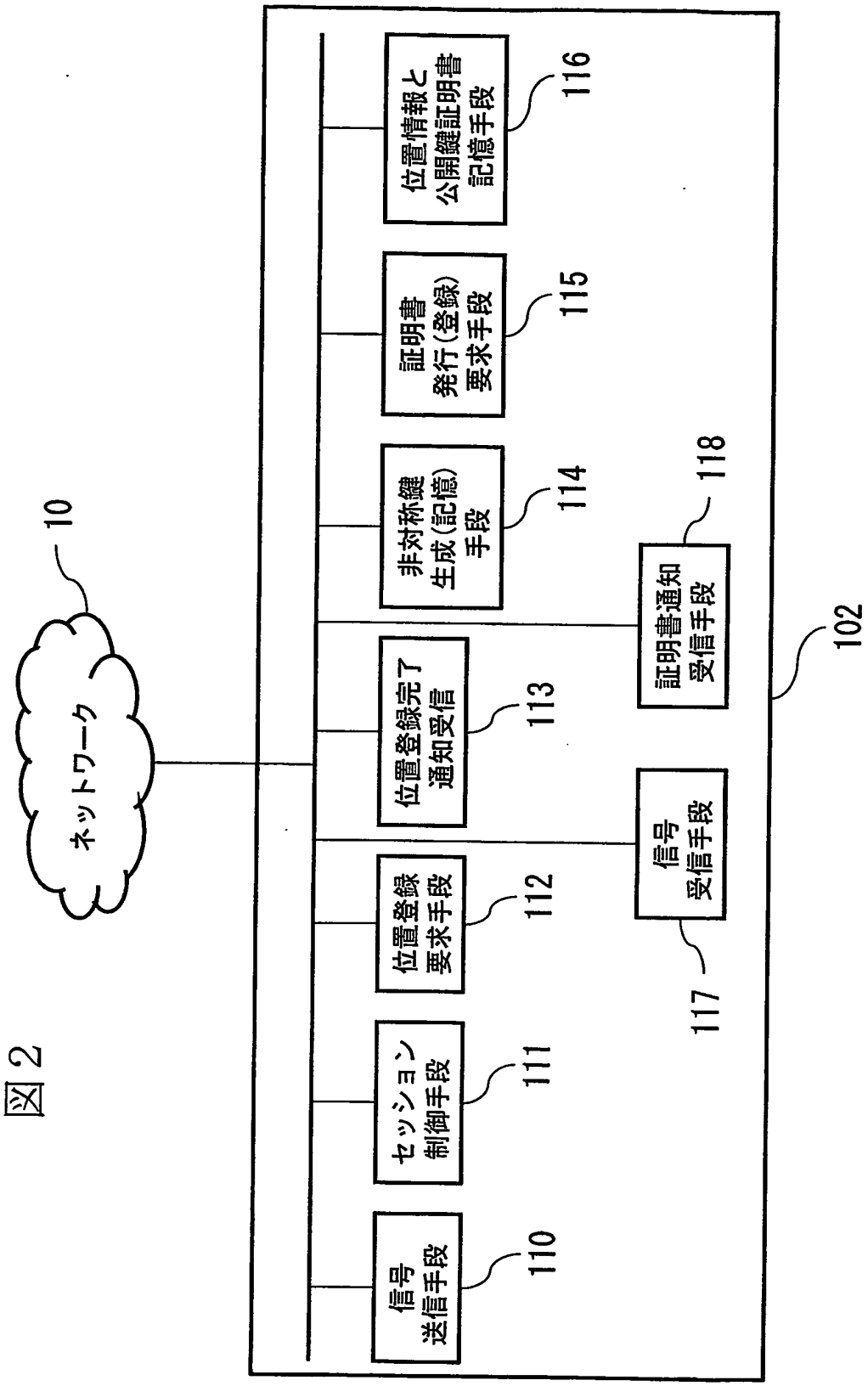

10
ネットワーク
102
信号送信手段
110
セッション制御手段
111
位置登録要求手段
112
位置登録完了通知受信
113
非対称鍵生成(記憶)手段
114
証明書発行(登録)要求手段
115
位置情報と公開鍵証明書記憶手段
116
信号受信手段
117
証明書通知受信手段
118

図2

図3

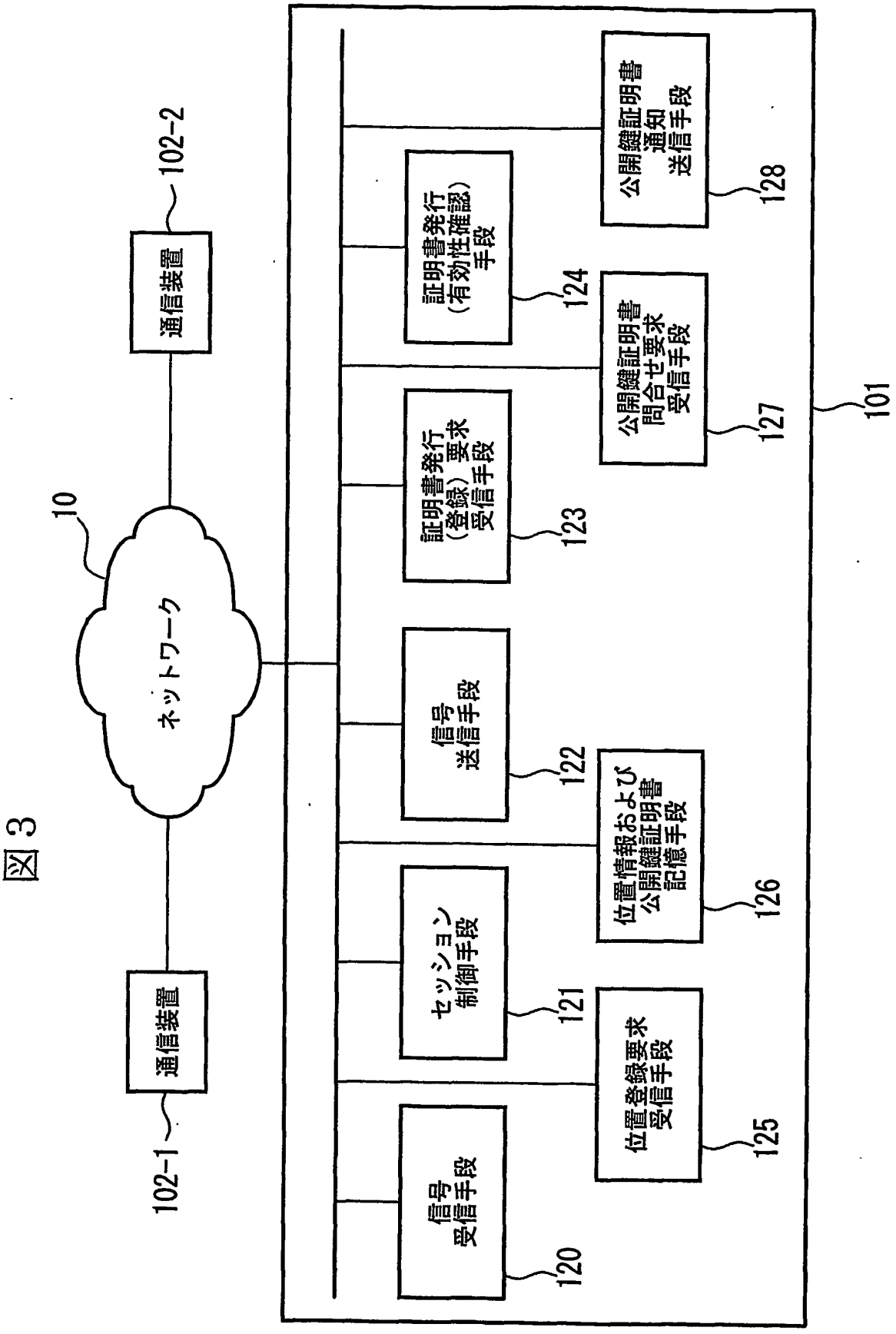

101
102-1
102-2
10
通信装置
通信装置
ネットワーク
信号
受信手段
120
セッション
制御手段
121
信号
送信手段
122
証明書発行
(登録)要求
受信手段
123
証明書発行
(有効性確認)
手段
124
位置登録要求
受信手段
125
位置情報および
公開鍵証明書
記憶手段
126
公開鍵証明書
問合せ要求
受信手段
127
公開鍵証明書
通知
送信手段
128

図4

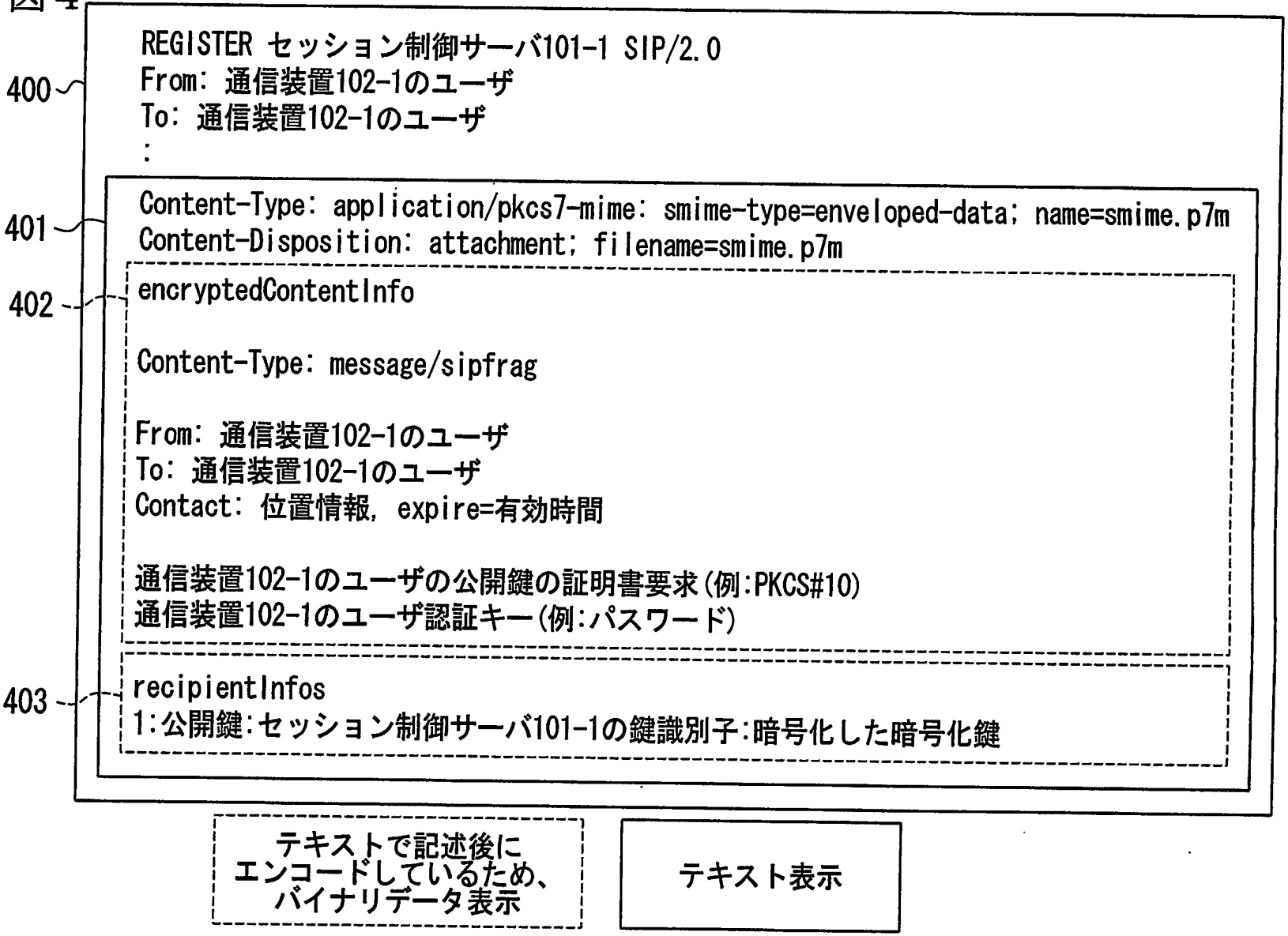

REGISTER セッション制御サーバ101-1 SIP/2.0
From: 通信装置102-1のユーザ
To: 通信装置102-1のユーザ
:
400
Content-Type: application/pkcs7-mime: smime-type=enveloped-data; name=smime.p7m
Content-Disposition: attachment; filename=smime.p7m
401
encryptedContentInfo
402
Content-Type: message/sipfrag
From: 通信装置102-1のユーザ
To: 通信装置102-1のユーザ
Contact: 位置情報, expire=有効時間
通信装置102-1のユーザの公開鍵の証明書要求(例:PKCS#10)
通信装置102-1のユーザ認証キー(例:パスワード)
recipientInfos
403
1:公開鍵:セッション制御サーバ101-1の鍵識別子:暗号化した暗号化鍵
テキストで記述後に
エンコードしているため、
バイナリデータ表示
テキスト表示

図5

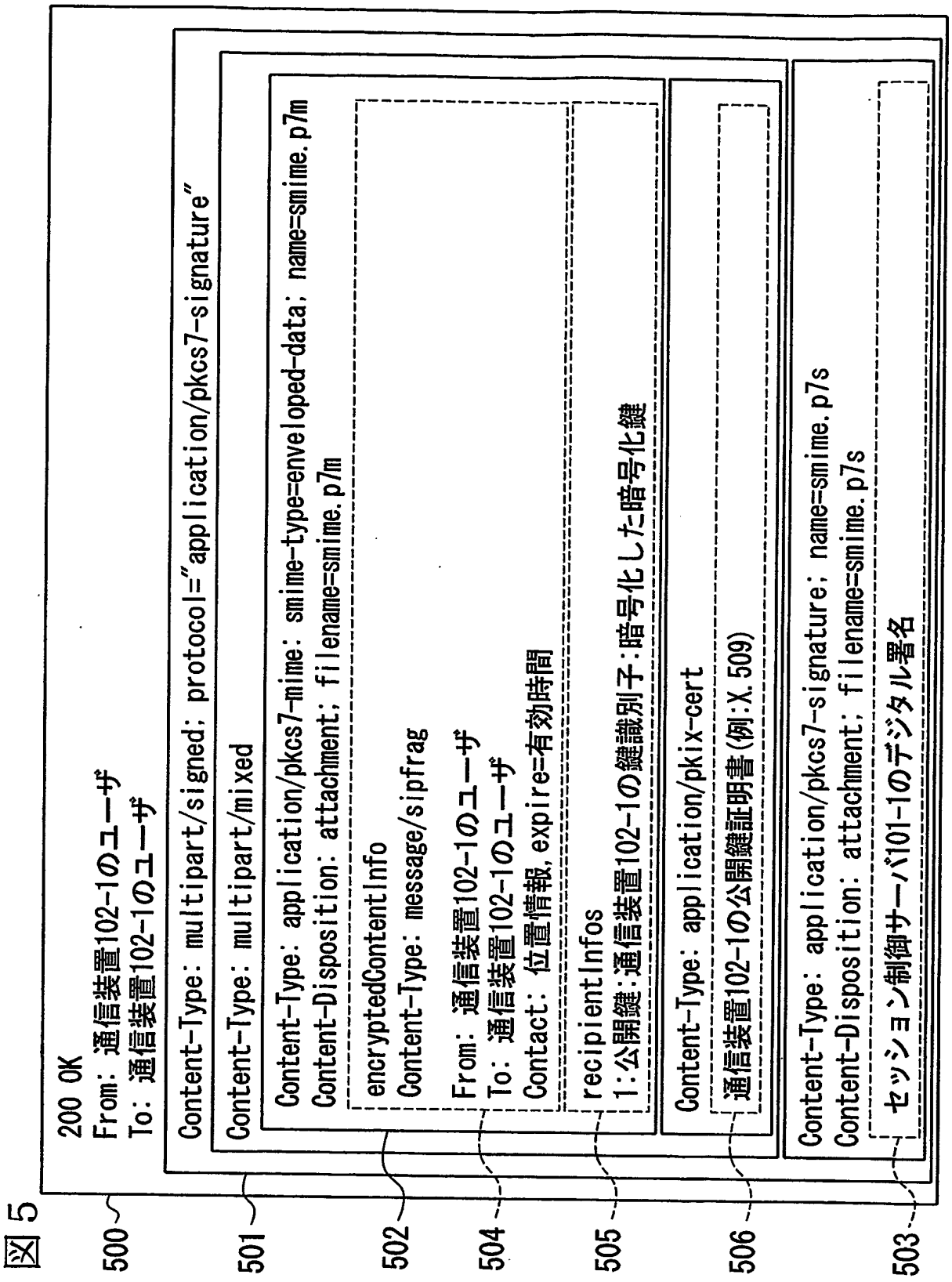

200 OK
From: 通信装置102-1のユーザ
To: 通信装置102-1のユーザ
Content-Type: multipart/signed; protocol="application/pkcs7-signature"
Content-Type: multipart/mixed
Content-Type: application/pkcs7-mime; smime-type=enveloped-data; name=smime.p7m
Content-Disposition: attachment; filename=smime.p7m
encryptedContentInfo
Content-Type: message/sipfrag
From: 通信装置102-1のユーザ
To: 通信装置102-1のユーザ
Contact: 位置情報, expire=有効時間
recipientInfos
1:公開鍵:通信装置102-1の鍵識別子:暗号化した暗号化鍵
Content-Type: application/pkix-cert
通信装置102-1の公開鍵証明書(例:X.509)
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Disposition: attachment; filename=smime.p7s
セッション制御サーバ101-1のデジタル署名
500
501
502
504
505
506
503

図 6

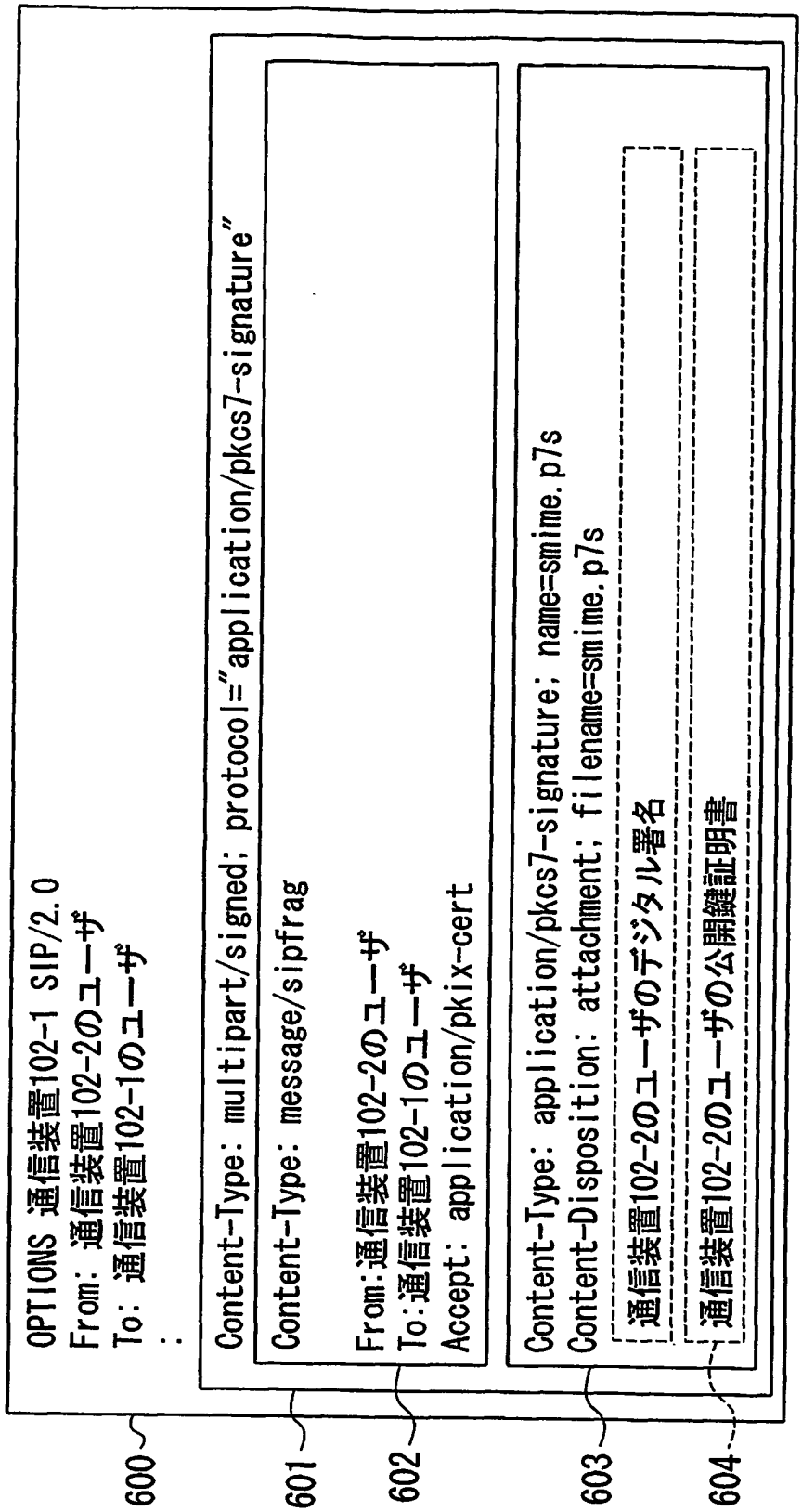

OPTIONS 通信装置102-1 SIP/2.0
From: 通信装置102-2のユーザ
To: 通信装置102-1のユーザ
:
Content-Type: multipart/signed; protocol="application/pkcs7-signature"
Content-Type: message/sipfrag
From:通信装置102-2のユーザ
To:通信装置102-1のユーザ
Accept: application/pkix-cert
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Disposition: attachment; filename=smime.p7s
通信装置102-2のユーザのデジタル署名
通信装置102-2のユーザの公開鍵証明書
600
601
602
603
604

図7

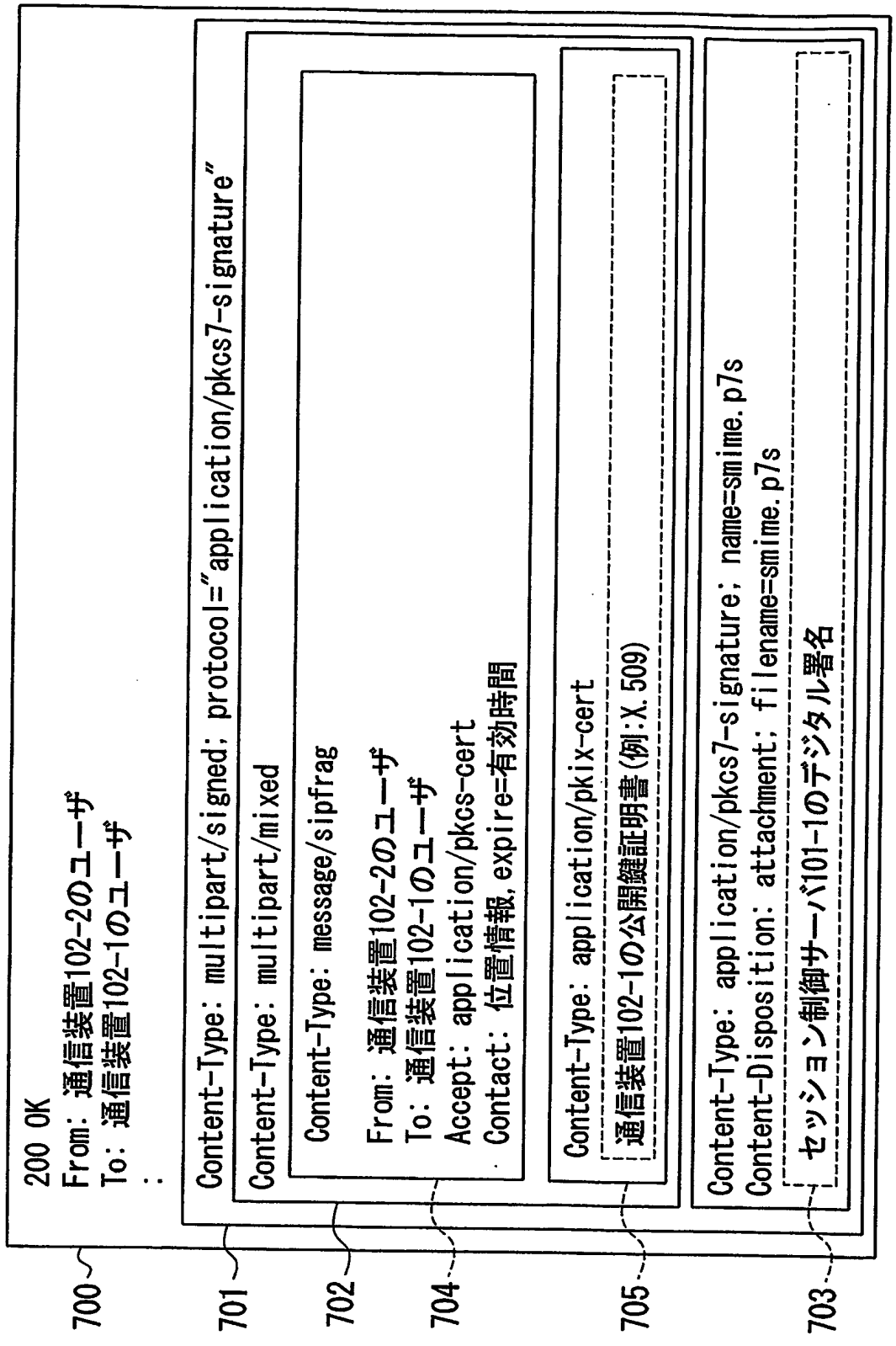
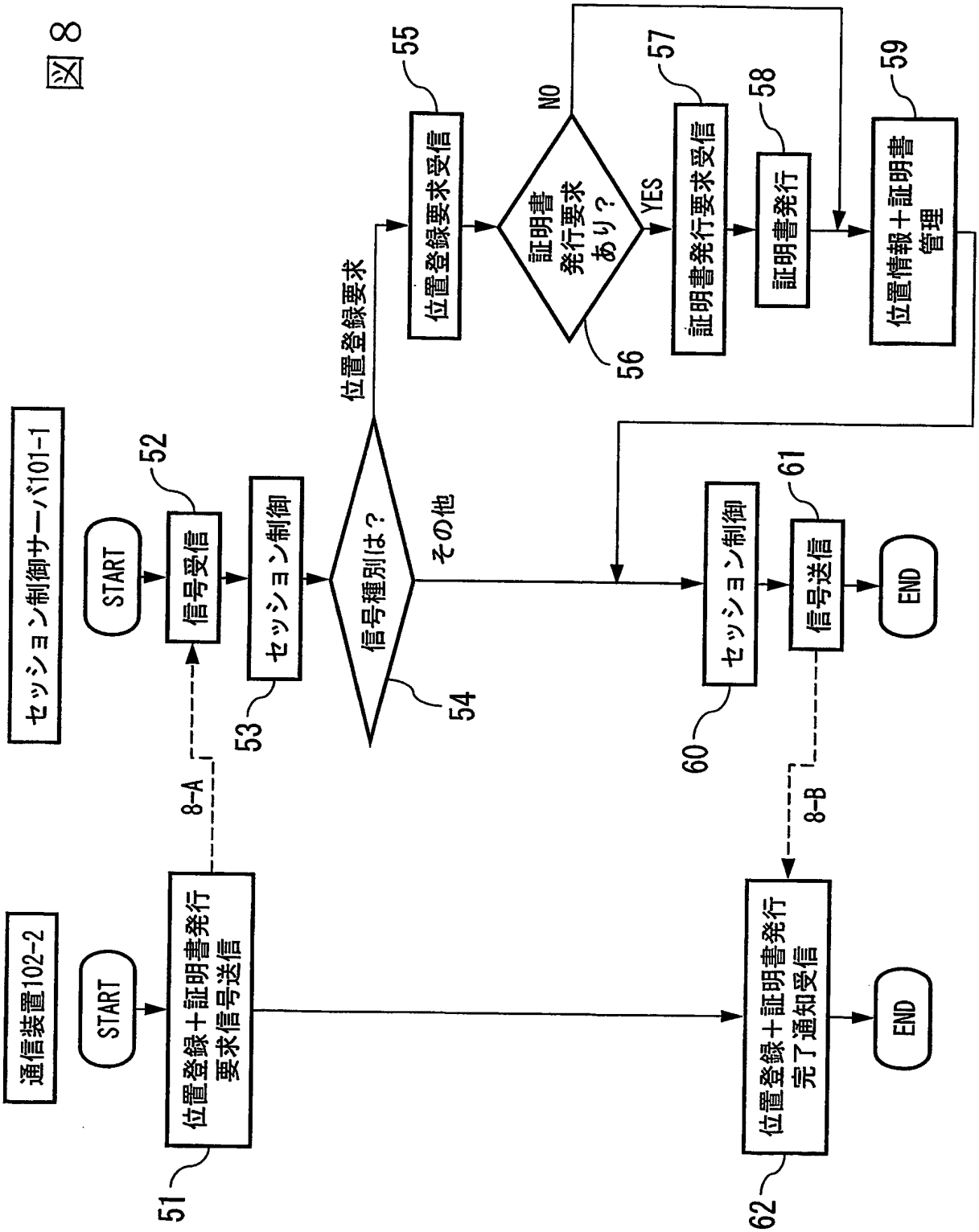

700
200 OK
From: 通信装置102-2のユーザ
To: 通信装置102-1のユーザ
:
701
Content-Type: multipart/signed; protocol="application/pkcs7-signature"
Content-Type: multipart/mixed
702
Content-Type: message/sipfrag
From: 通信装置102-2のユーザ
To: 通信装置102-1のユーザ
Accept: application/pkcs-cert
Contact: 位置情報, expire=有効時間
704
Content-Type: application/pkix-cert
通信装置102-1の公開鍵証明書(例:X.509)
705
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Disposition: attachment; filename=smime.p7s
セッション制御サーバ101-1のデジタル署名
703

図8


通信装置102-2
START
位置登録＋証明書発行
要求信号送信
51
8-A
セッション制御サーバ101-1
START
信号受信
52
セッション制御
53
信号種別は？
54
位置登録要求
その他
位置登録要求受信
55
証明書
発行要求
あり？
56
NO
YES
証明書発行要求受信
57
証明書発行
58
位置情報＋証明書
管理
59
セッション制御
60
信号送信
61
END
8-B
位置登録＋証明書発行
完了通知受信
62
END

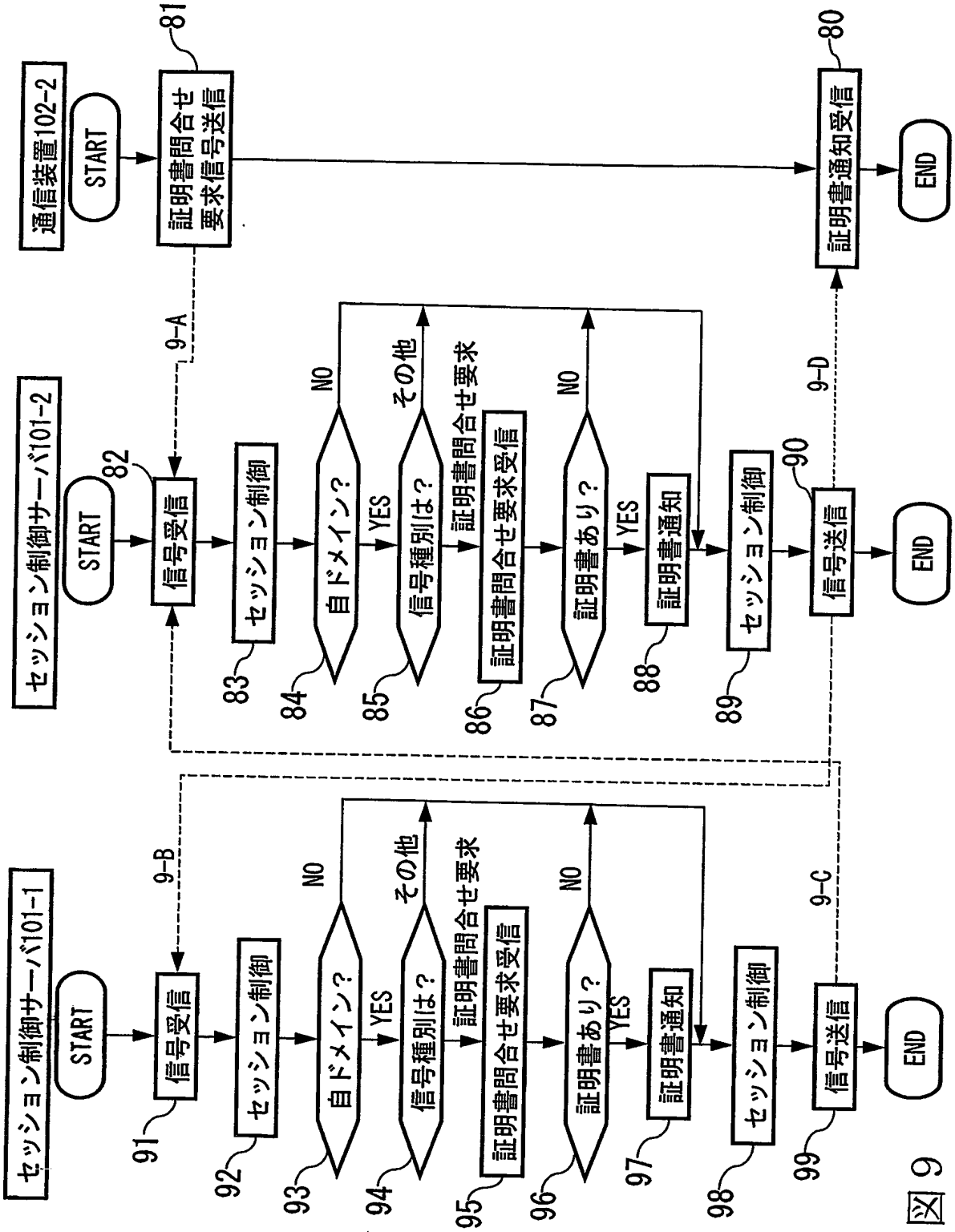

通信装置102-2
START
81
証明書問合せ要求信号送信
80
証明書通知受信
END
9-A
9-D
セッションコントロールサーバ101-2
START
82
信号受信
83
セッション制御
84
自ドメイン?
NO
YES
85
信号種別は?
その他
86
証明書問合せ要求受信
87
証明書あり?
NO
YES
88
証明書通知
89
セッション制御
90
信号送信
END
9-B
9-C
セッションコントロールサーバ101-1
START
91
信号受信
92
セッション制御
93
自ドメイン?
NO
YES
94
信号種別は?
その他
95
証明書問合せ要求受信
96
証明書あり?
NO
YES
97
証明書通知
98
セッション制御
99
信号送信
END

図9

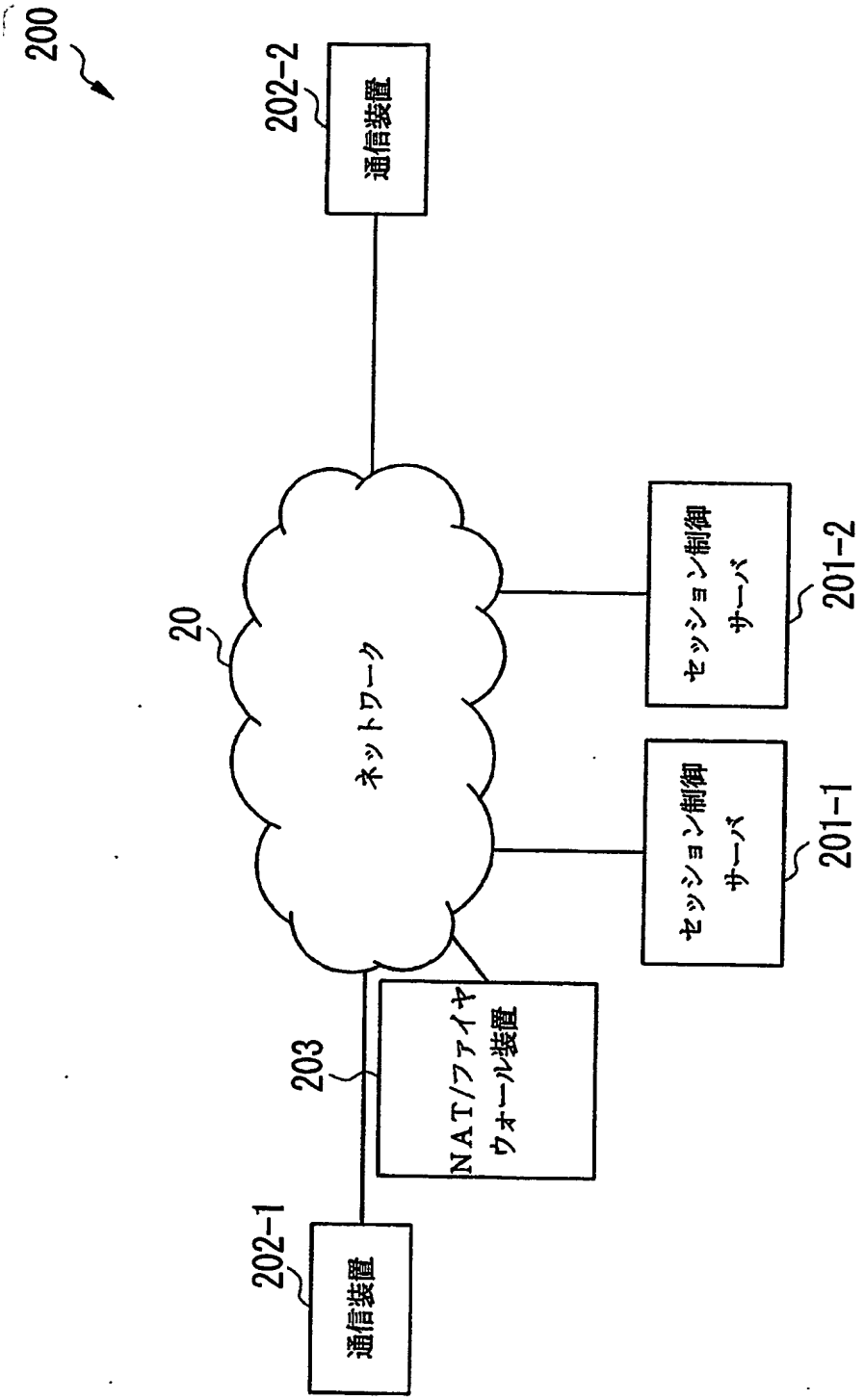

200
202-2
通信装置
20
ネットワーク
セッション制御
サーバ
201-2
セッション制御
サーバ
201-1
203
NAT/ファイヤ
ウォール装置
202-1
通信装置

図１０

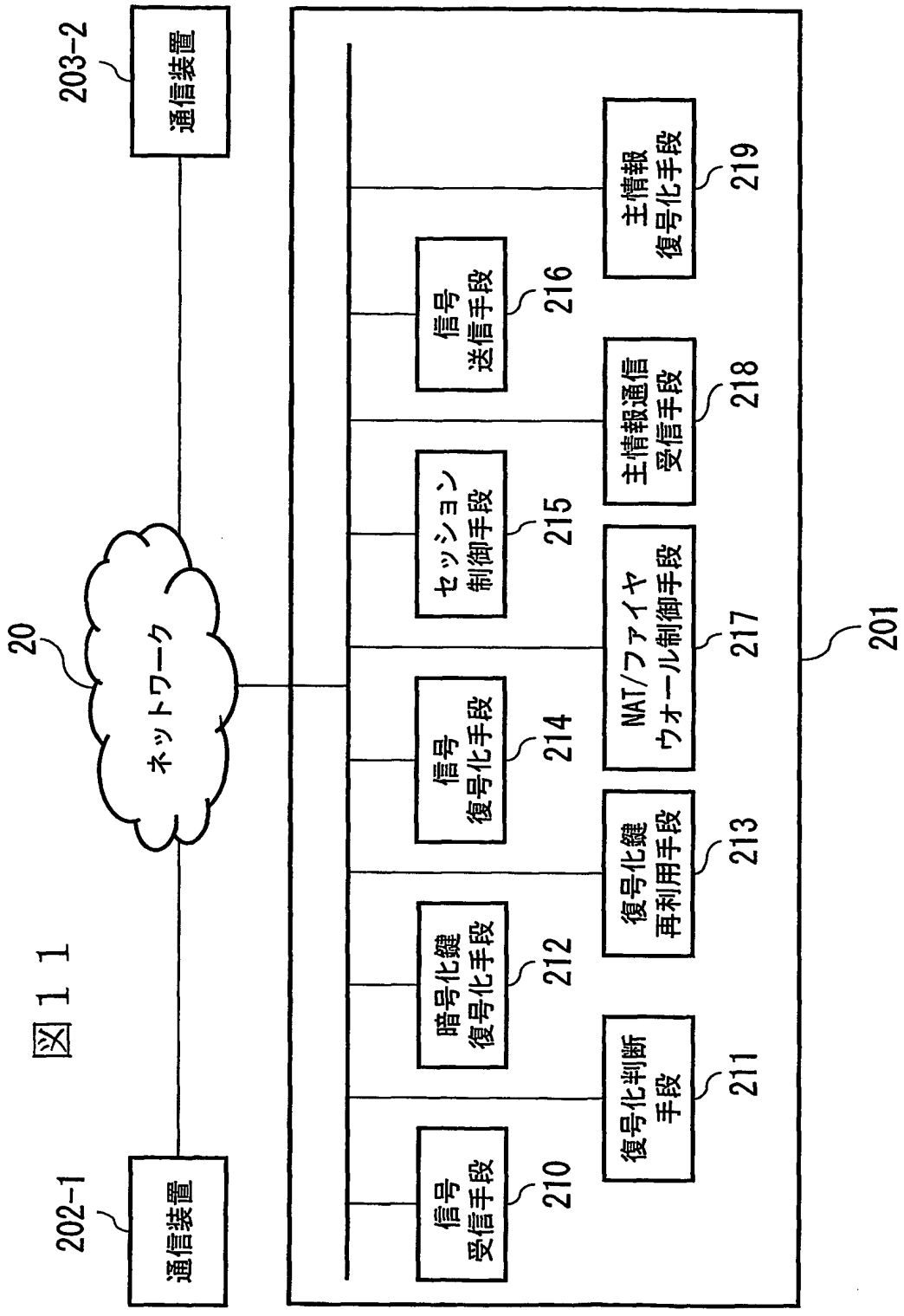

203-2
通信装置
20
ネットワーク
202-1
通信装置
201
信号
受信手段
210
復号化判断
手段
211
暗号化鍵
復号化手段
212
復号化鍵
再利用手段
213
信号
復号化手段
214
NAT/ファイヤ
ウォール制御手段
217
セッション
制御手段
215
主情報通信
受信手段
218
信号
送信手段
216
主情報
復号化手段
219

図１１

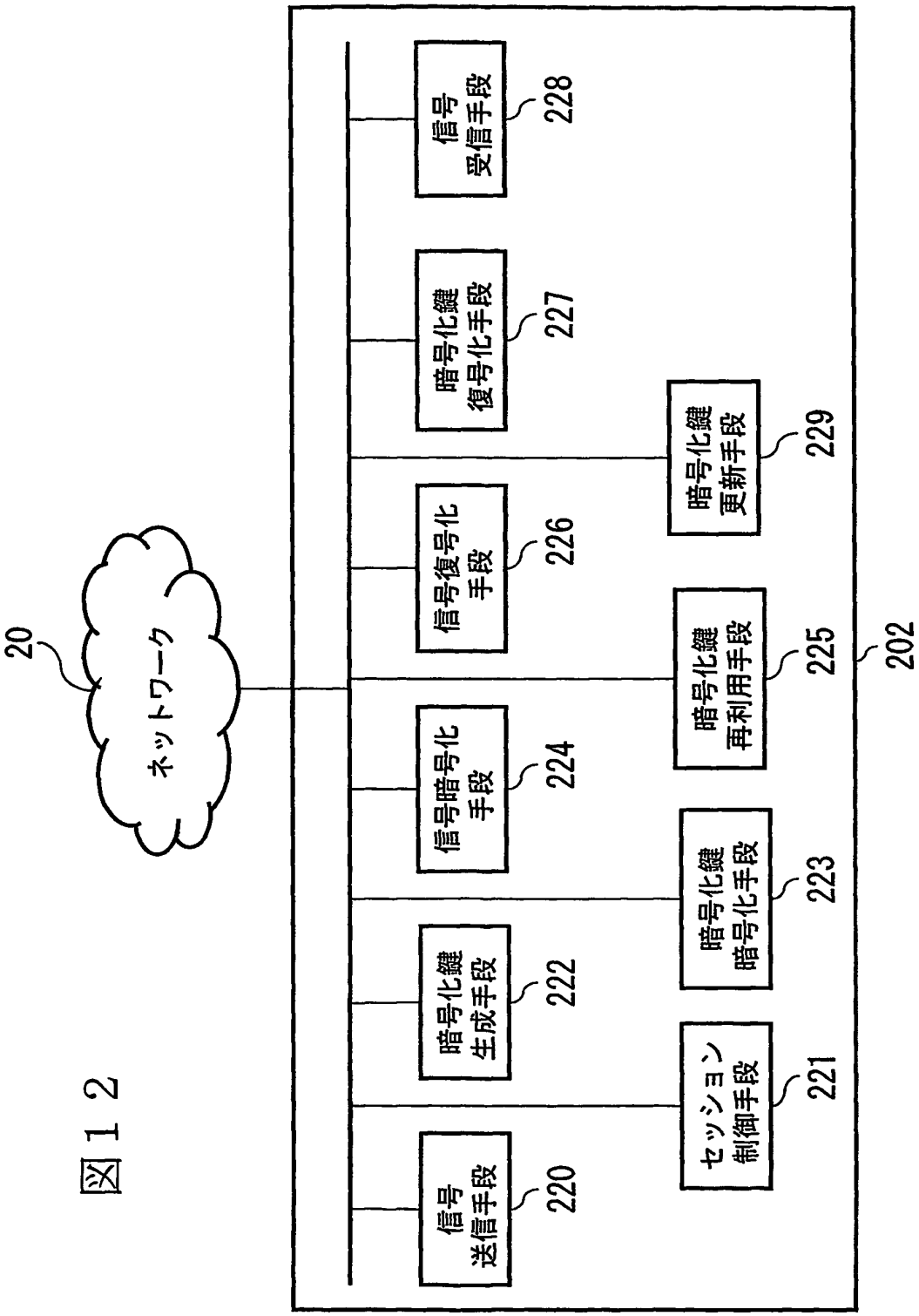

20
ネットワーク
202
信号送信手段
220
セッション制御手段
221
暗号化鍵生成手段
222
暗号化鍵暗号化手段
223
信号暗号化手段
224
暗号化鍵再利用手段
225
信号復号化手段
226
暗号化鍵復号化手段
227
信号受信手段
228
暗号化鍵更新手段
229

図１２

図13

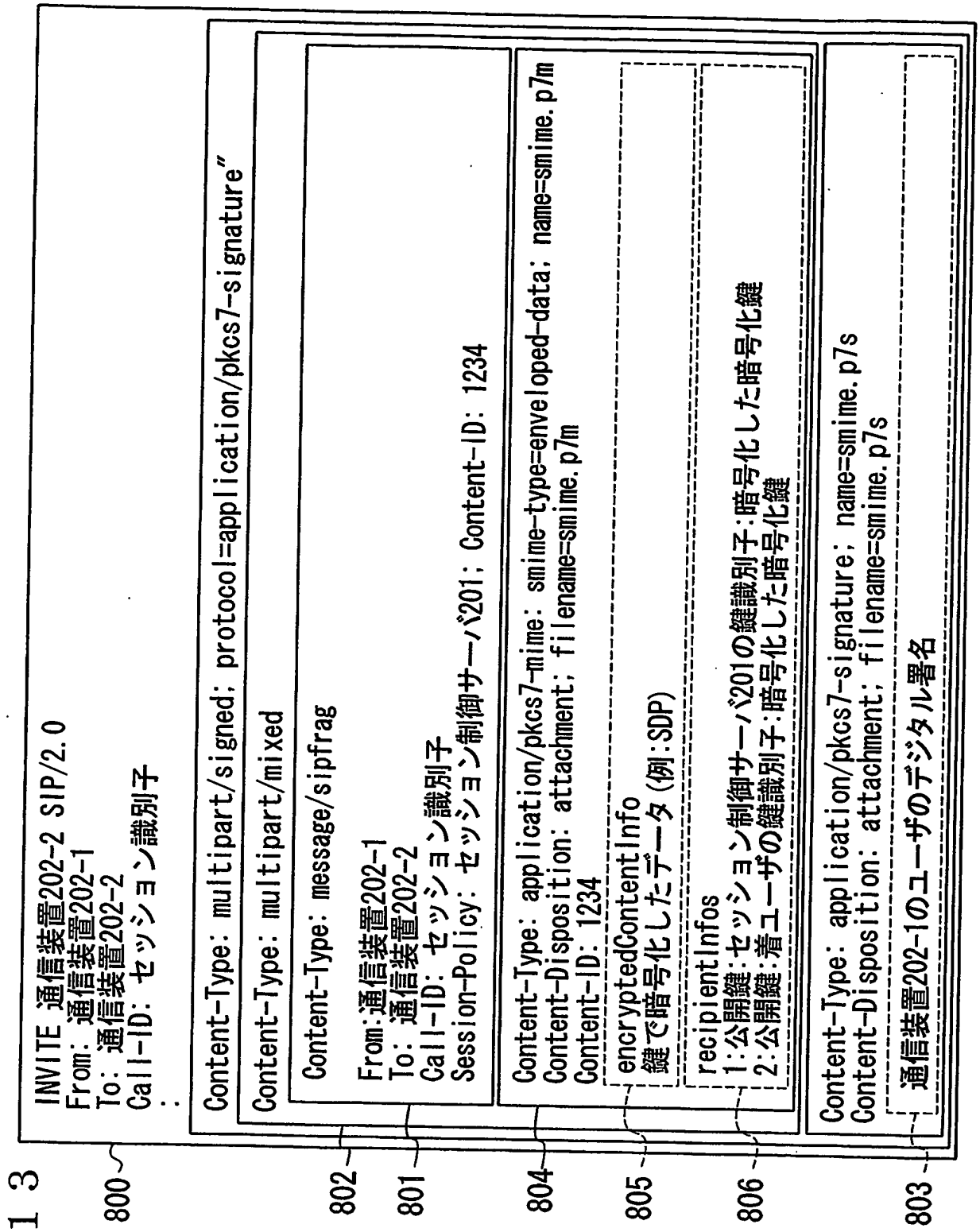

INVITE 通信装置202-2 SIP/2.0
From: 通信装置202-1
To: 通信装置202-2
Call-ID: セッション識別子
...
800
Content-Type: multipart/signed; protocol=application/pkcs7-signature"
Content-Type: multipart/mixed
802
Content-Type: message/sipfrag
From:通信装置202-1
To: 通信装置202-2
Call-ID: セッション識別子
Session-Policy: セッション制御サーバ201; Content-ID: 1234
801
Content-Type: application/pkcs7-mime; smime-type=enveloped-data; name=smime.p7m
Content-Disposition: attachment; filename=smime.p7m
Content-ID: 1234
804
encryptedContentInfo
鍵で暗号化したデータ(例:SDP)
805
recipientInfos
1:公開鍵:セッション制御サーバ201の鍵識別子:暗号化した暗号化鍵
2:公開鍵:着ユーザの鍵識別子:暗号化した暗号化鍵
806
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Disposition: attachment; filename=smime.p7s
803
通信装置202-1のユーザのデジタル署名

図14

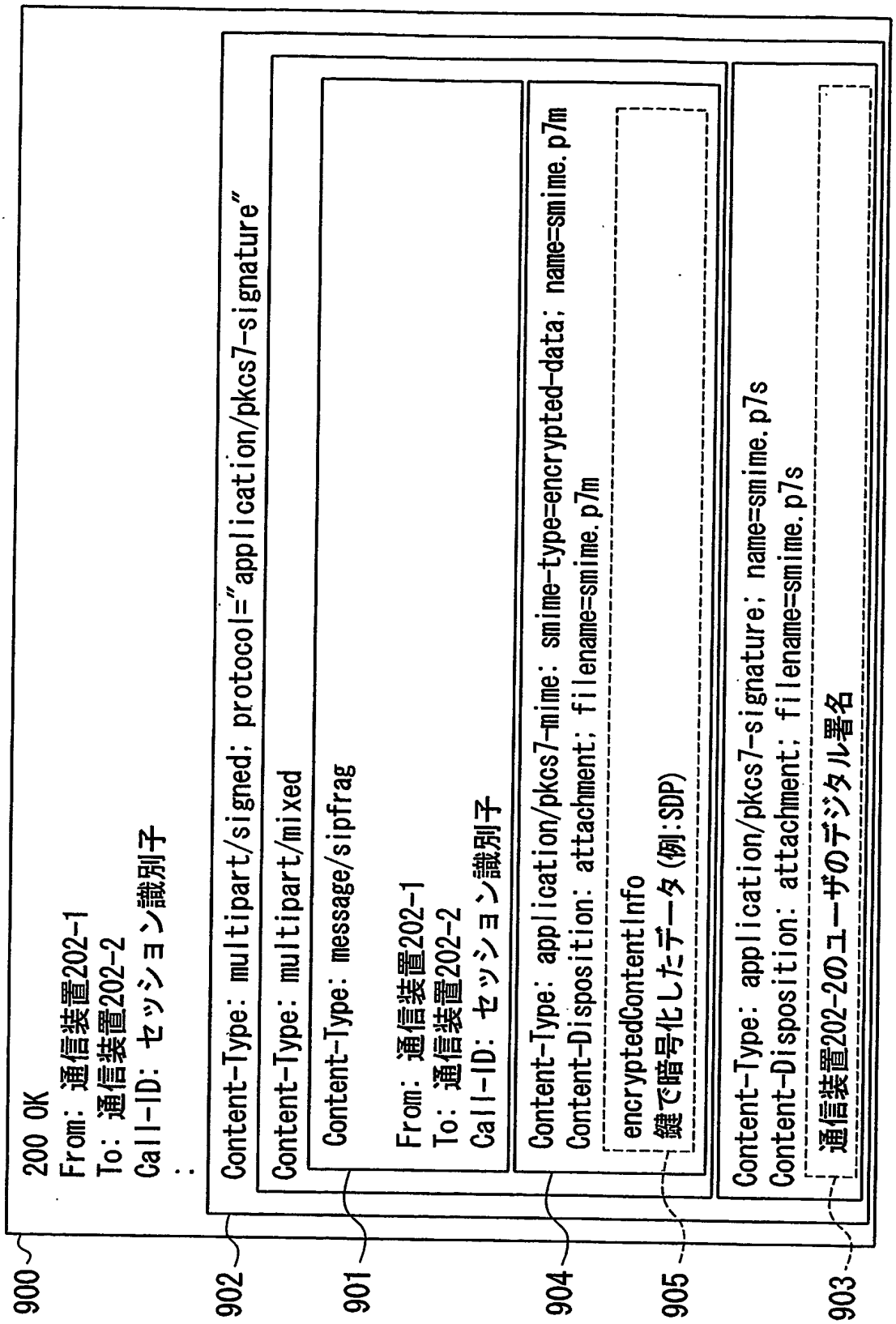

900
200 OK
From: 通信装置202-1
To: 通信装置202-2
Call-ID: セッション識別子
:
902
Content-Type: multipart/signed; protocol="application/pkcs7-signature"
901
Content-Type: multipart/mixed
Content-Type: message/sipfrag
From: 通信装置202-1
To: 通信装置202-2
Call-ID: セッション識別子
904
Content-Type: application/pkcs7-mime; smime-type=encrypted-data; name=smime.p7m
Content-Disposition: attachment; filename=smime.p7m
905
encryptedContentInfo
鍵で暗号化したデータ(例:SDP)
903
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Disposition: attachment; filename=smime.p7s
通信装置202-2のユーザのデジタル署名

図15

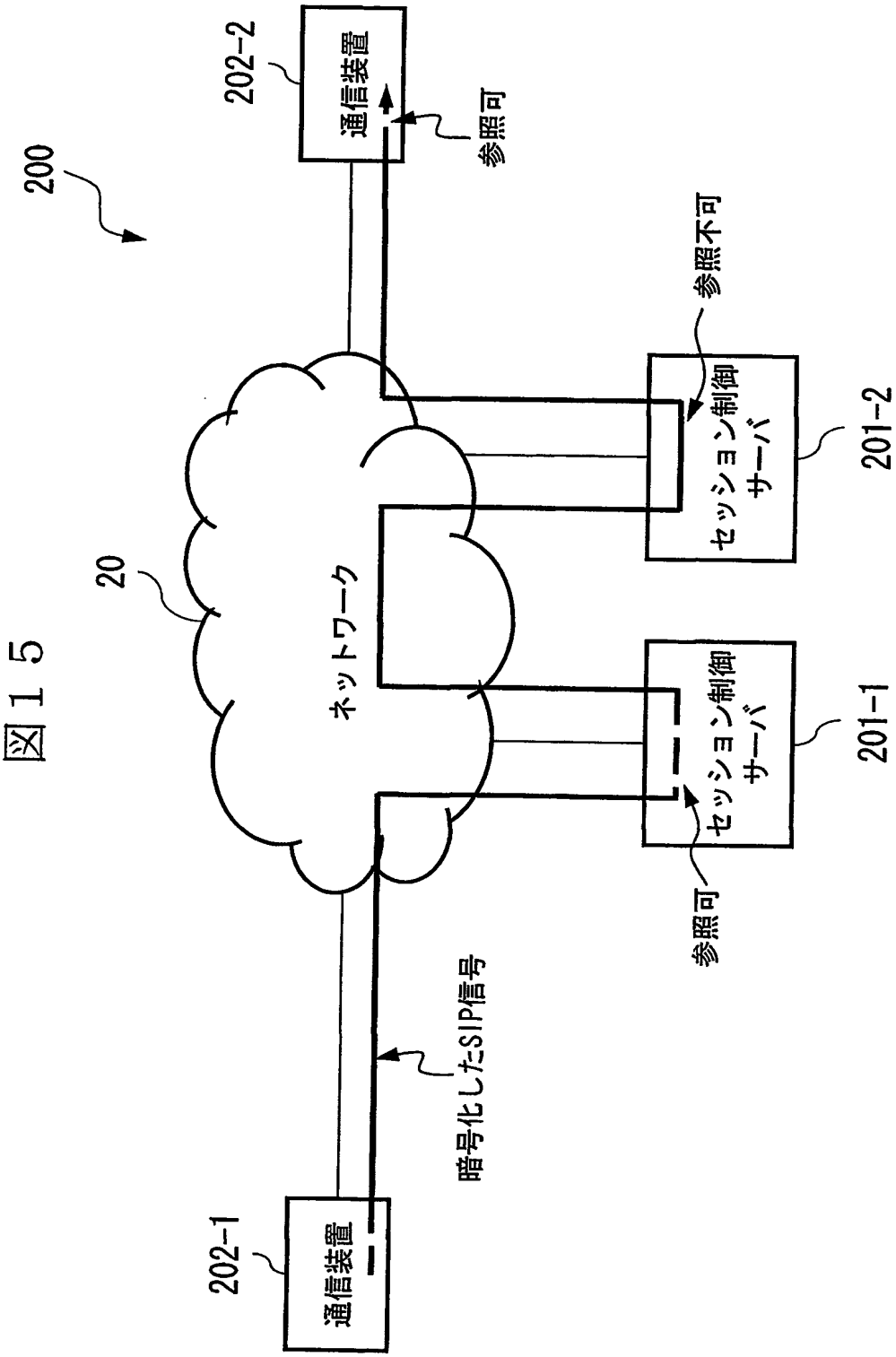

200
202-2
通信装置
参照可
参照不可
セッション制御
サーバ
201-2
20
ネットワーク
セッション制御
サーバ
201-1
参照可
暗号化したSIP信号
202-1
通信装置

図１６

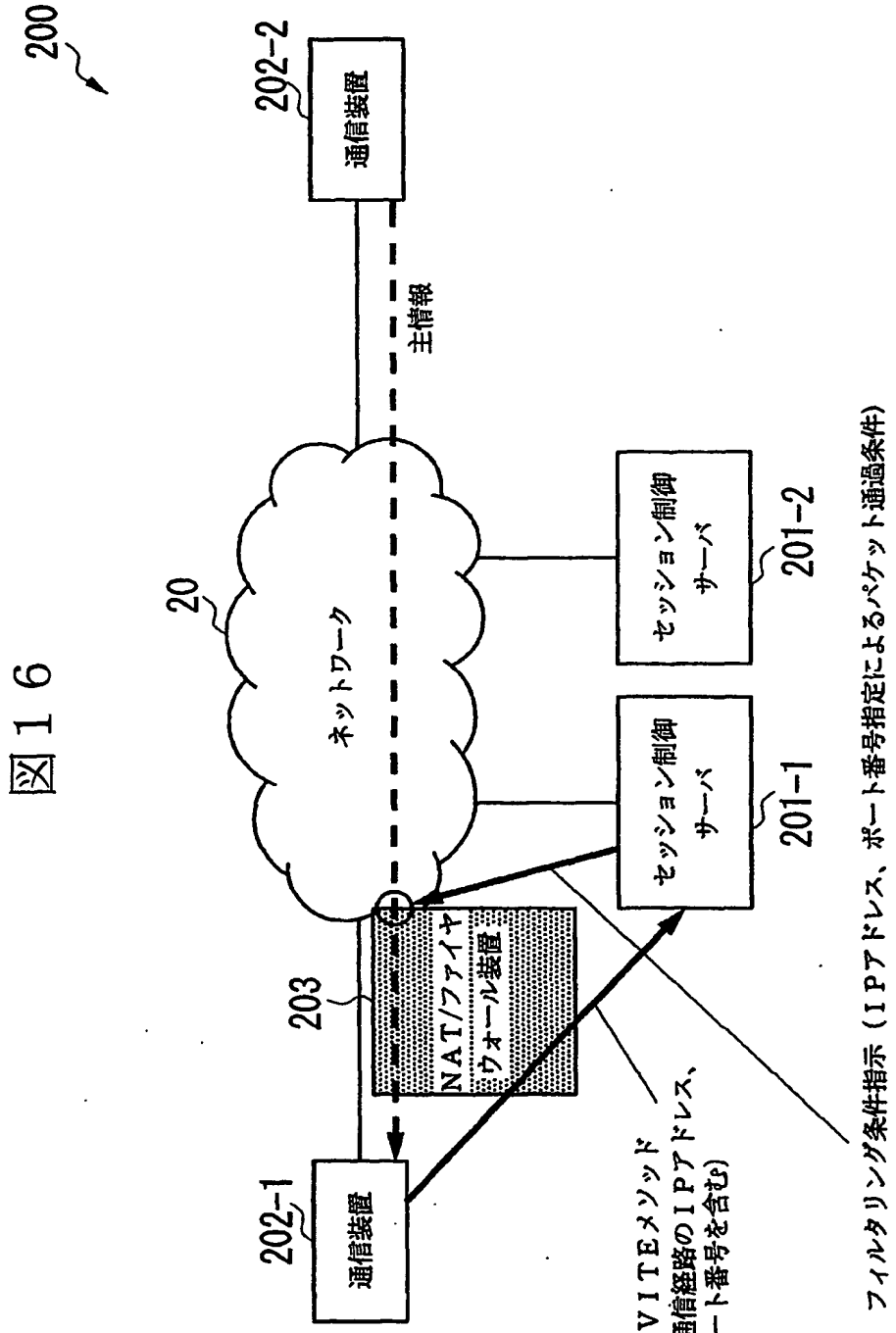

200
202-2
通信装置
主情報
20
ネットワーク
セッション制御
サーバ
201-2
セッション制御
サーバ
201-1
203
NAT/ファイヤ
ウォール装置
202-1
通信装置
INVITEメソッド
(主情報通信経路のIPアドレス、
ポート番号を含む)
フィルタリング条件指示（IPアドレス、ポート番号指定によるパケット通過条件）

図17

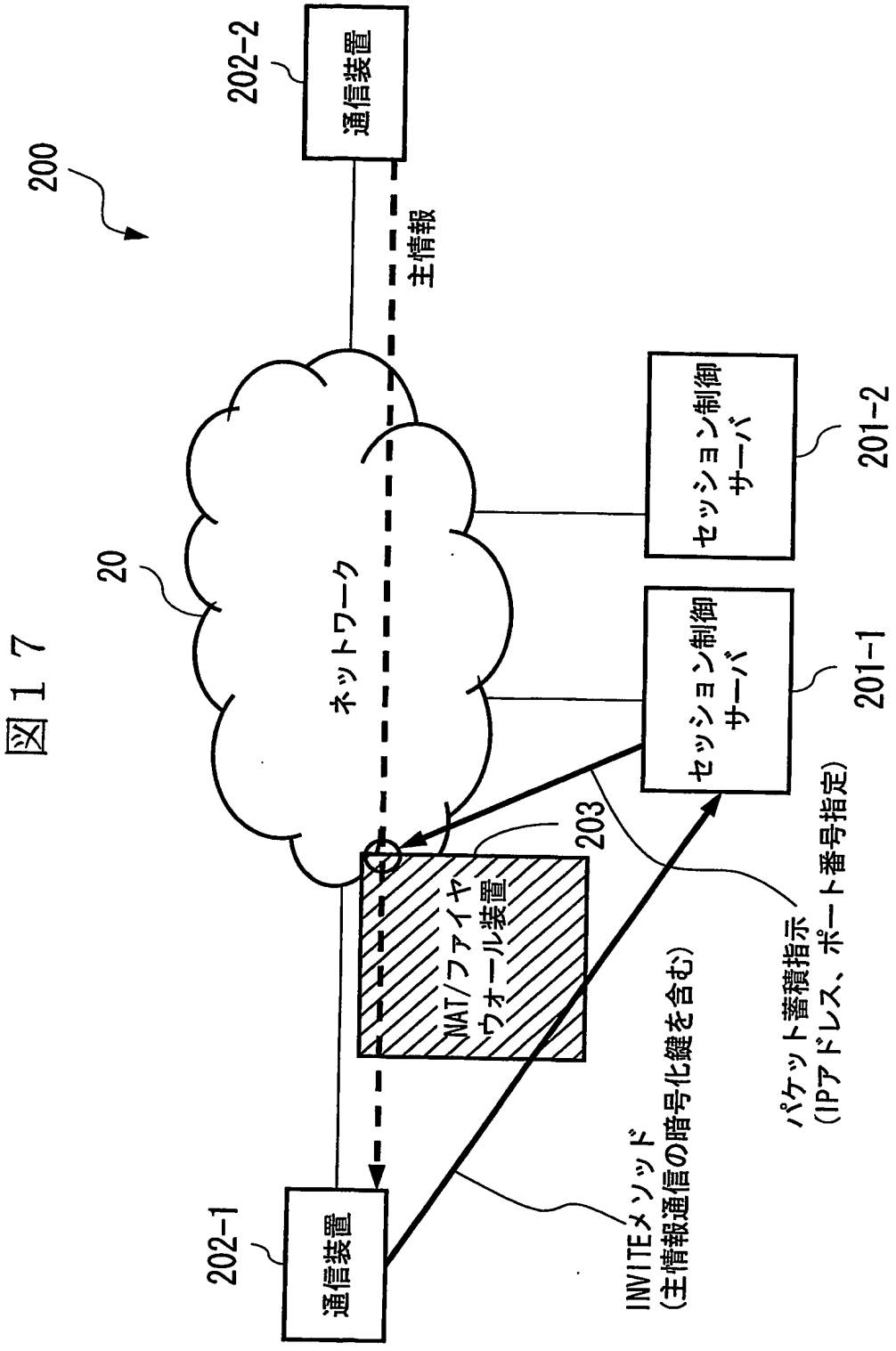
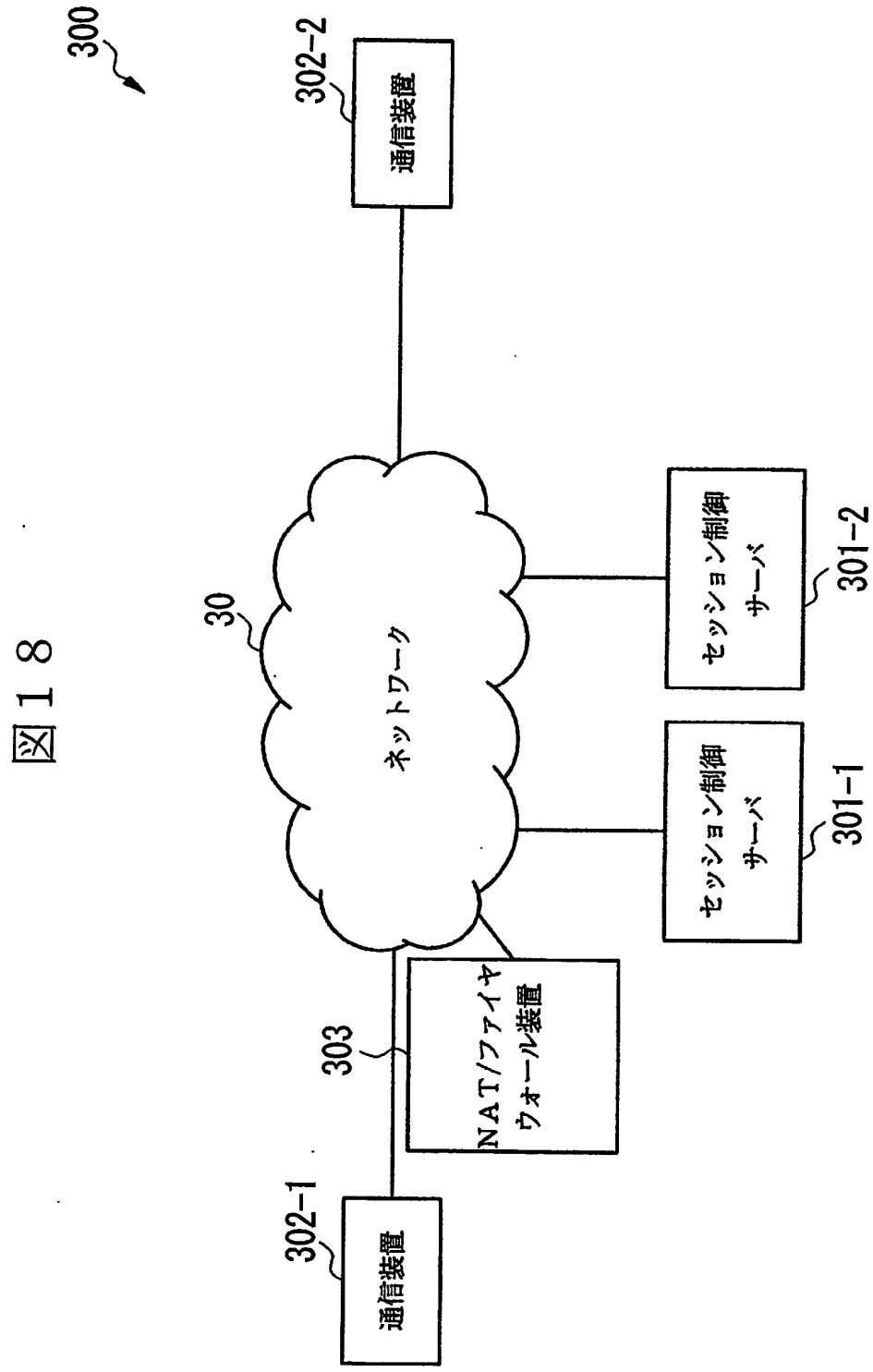

200
202-2
通信装置
主情報
20
ネットワーク
セッション制御
サーバ
201-2
セッション制御
サーバ
201-1
203
NAT/ファイヤ
ウォール装置
パケット蓄積指示
(IPアドレス、ポート番号指定)
INVITEメソッド
(主情報通信の暗号化鍵を含む)
202-1
通信装置

図１８


300
302-2
通信装置
30
ネットワーク
セッション制御サーバ
301-2
セッション制御サーバ
301-1
303
NAT/ファイヤウォール装置
302-1
通信装置

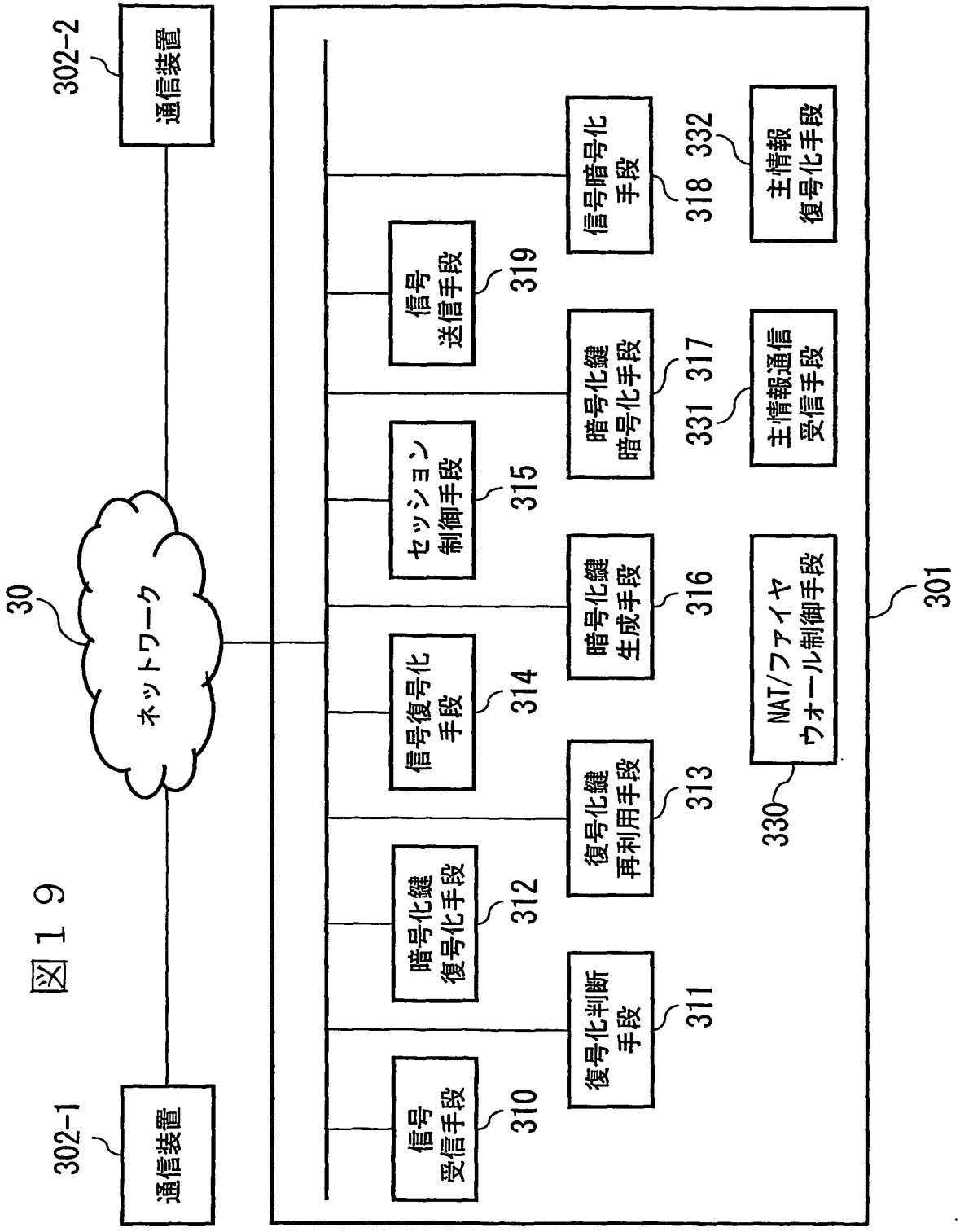

302-2
通信装置
30
ネットワーク
302-1
通信装置
信号受信手段
310
復号化判断手段
311
暗号化鍵復号化手段
312
復号化鍵再利用手段
313
信号復号化手段
314
暗号化鍵生成手段
316
セッション制御手段
315
暗号化鍵暗号化手段
331 317
信号送信手段
319
信号暗号化手段
318 332
主情報復号化手段
主情報通信受信手段
NAT/ファイヤウォール制御手段
330
301

図19

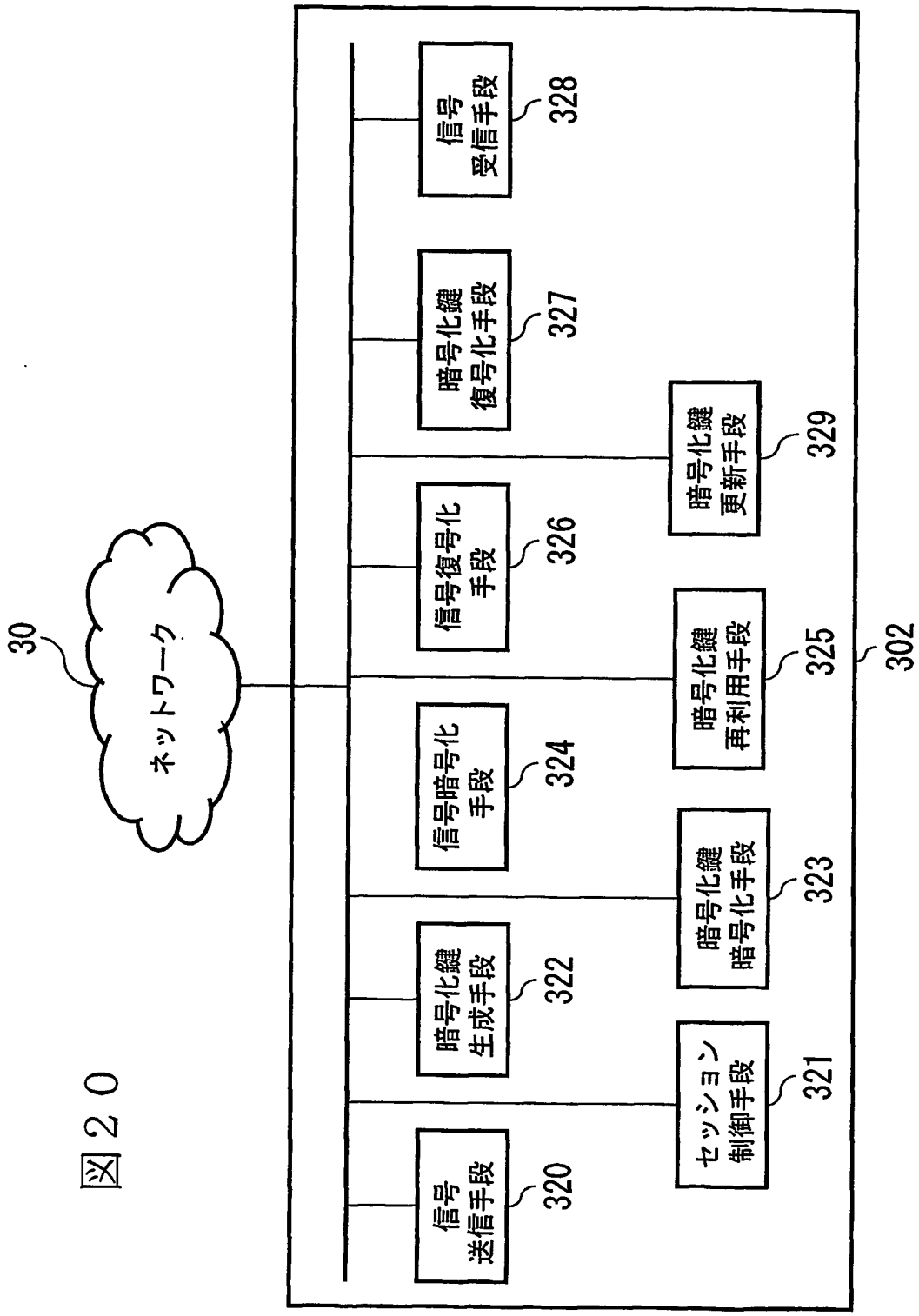

30
ネットワーク
302
信号送信手段
320
暗号化鍵生成手段
322
信号暗号化手段
324
信号復号化手段
326
暗号化鍵復号化手段
327
信号受信手段
328
セッション制御手段
321
暗号化鍵暗号化手段
323
暗号化鍵再利用手段
325
暗号化鍵更新手段
329

図２０

図２１

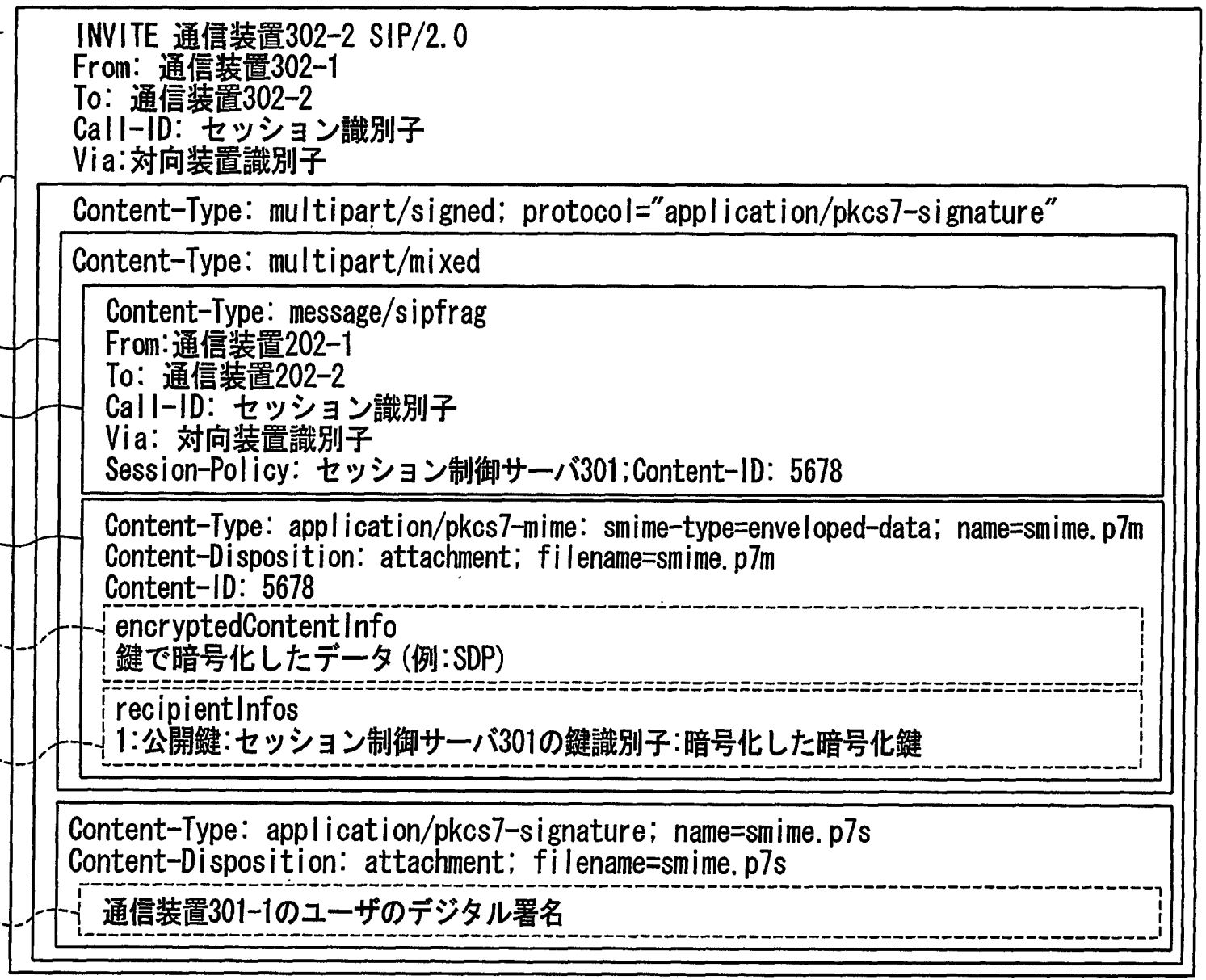

INVITE 通信装置302-2 SIP/2.0
From: 通信装置302-1
To: 通信装置302-2
Call-ID: セッション識別子
Via:対向装置識別子
1000
Content-Type: multipart/signed; protocol="application/pkcs7-signature"
Content-Type: multipart/mixed
Content-Type: message/sipfrag
From:通信装置202-1
To: 通信装置202-2
Call-ID: セッション識別子
Via: 対向装置識別子
Session-Policy: セッション制御サーバ301;Content-ID: 5678
1002
1001
Content-Type: application/pkcs7-mime: smime-type=enveloped-data; name=smime.p7m
Content-Disposition: attachment; filename=smime.p7m
Content-ID: 5678
1004
encryptedContentInfo
鍵で暗号化したデータ(例:SDP)
1005
recipientInfos
1:公開鍵:セッション制御サーバ301の鍵識別子:暗号化した暗号化鍵
1006
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Disposition: attachment; filename=smime.p7s
通信装置301-1のユーザのデジタル署名
1003

図22

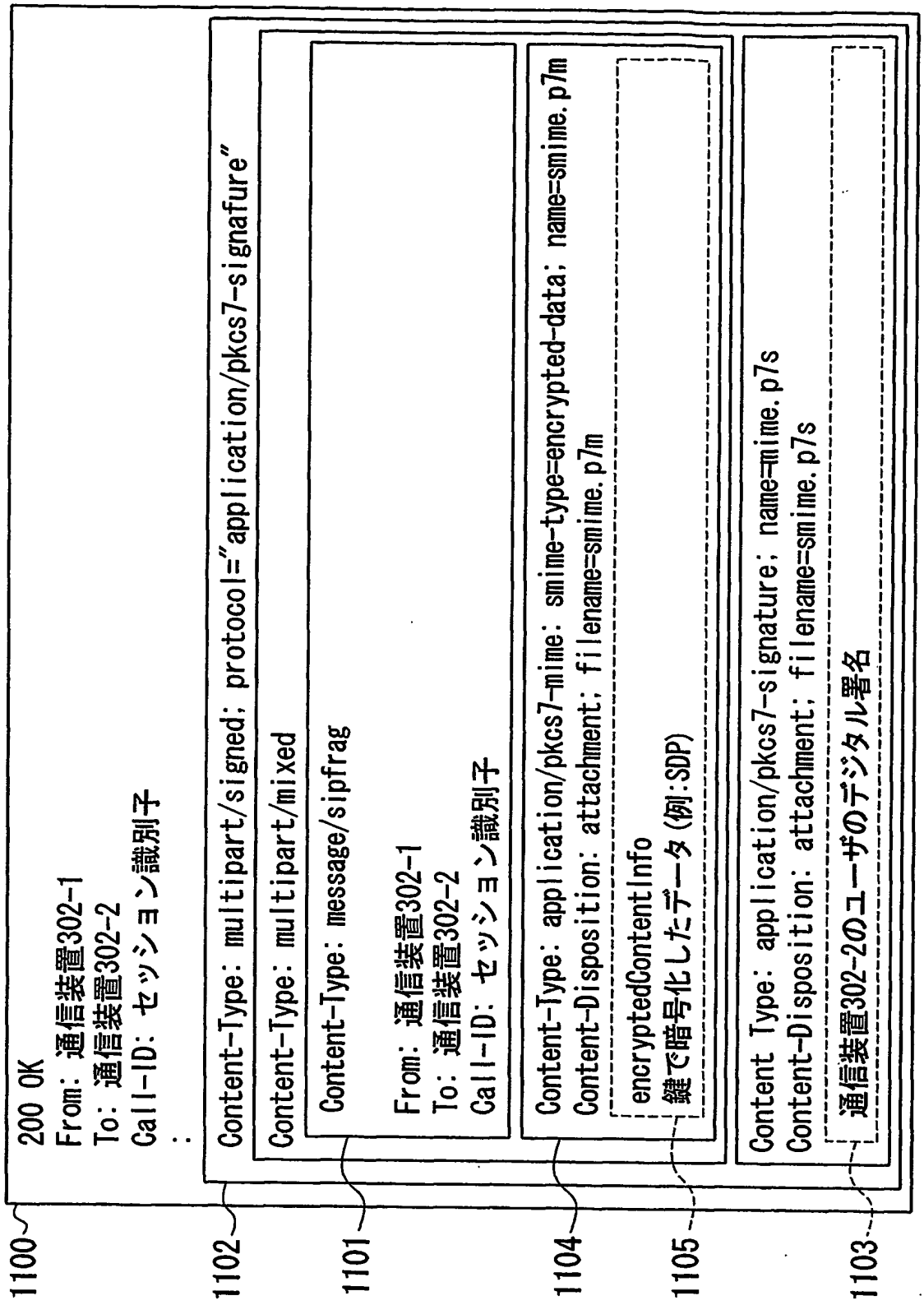

1100
200 OK
From: 通信装置302-1
To: 通信装置302-2
Call-ID: セッション識別子
:
1102
Content-Type: multipart/signed; protocol="application/pkcs7-signature"
1101
Content-Type: multipart/mixed
Content-Type: message/sipfrag
From: 通信装置302-1
To: 通信装置302-2
Call-ID: セッション識別子
1104
Content-Type: application/pkcs7-mime; smime-type=encrypted-data; name=smime.p7m
Content-Disposition: attachment; filename=smime.p7m
1105
encryptedContentInfo
鍵で暗号化したデータ(例:SDP)
1103
Content Type: application/pkcs7-signature; name=mime.p7s
Content-Disposition: attachment; filename=smime.p7s
通信装置302-2のユーザのデジタル署名

図２３

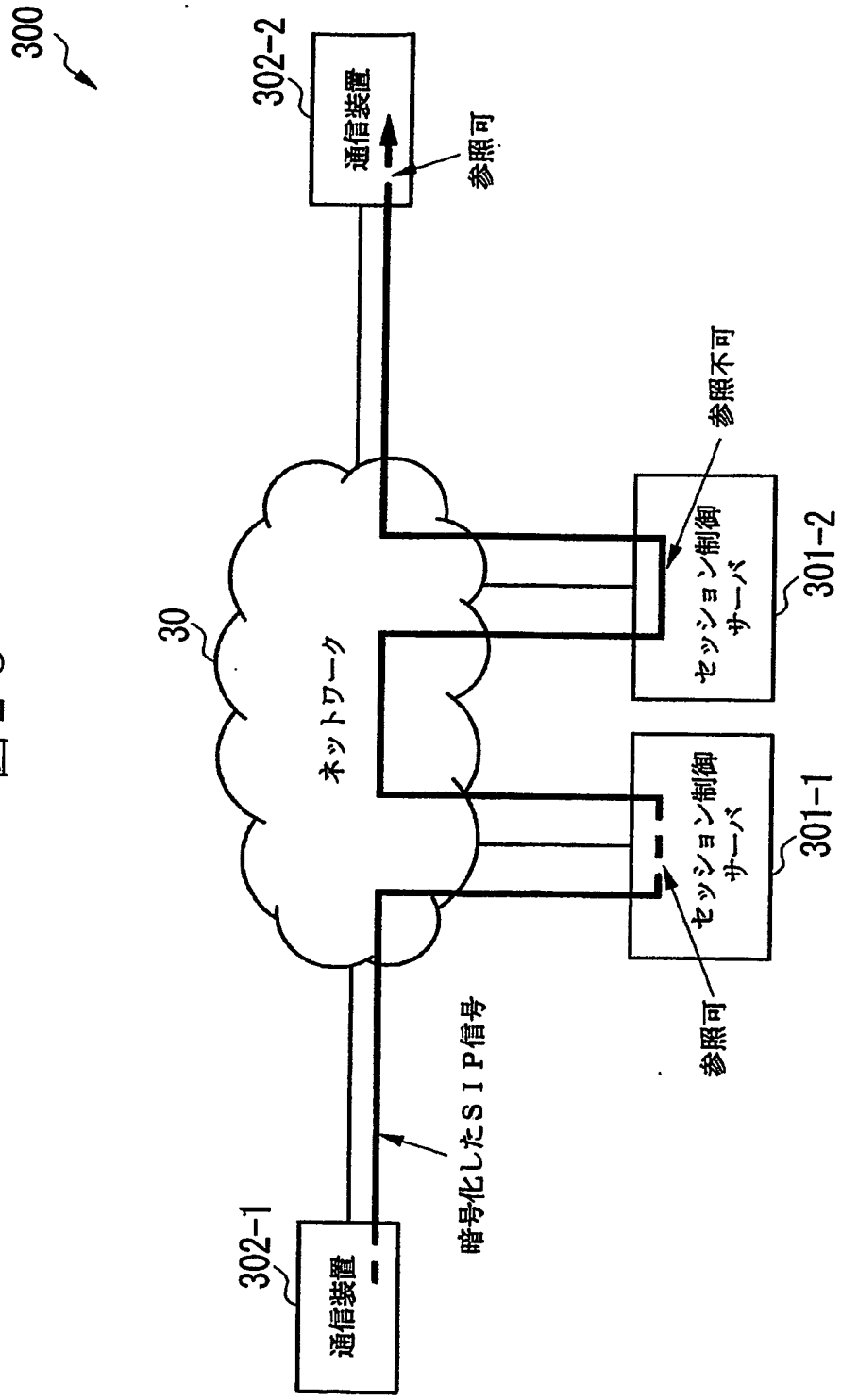

300
302-2
通信装置
参照可
参照不可
30
ネットワーク
セッション制御
サーバ
301-2
セッション制御
サーバ
301-1
参照可
暗号化したＳＩＰ信号
302-1
通信装置

図２４

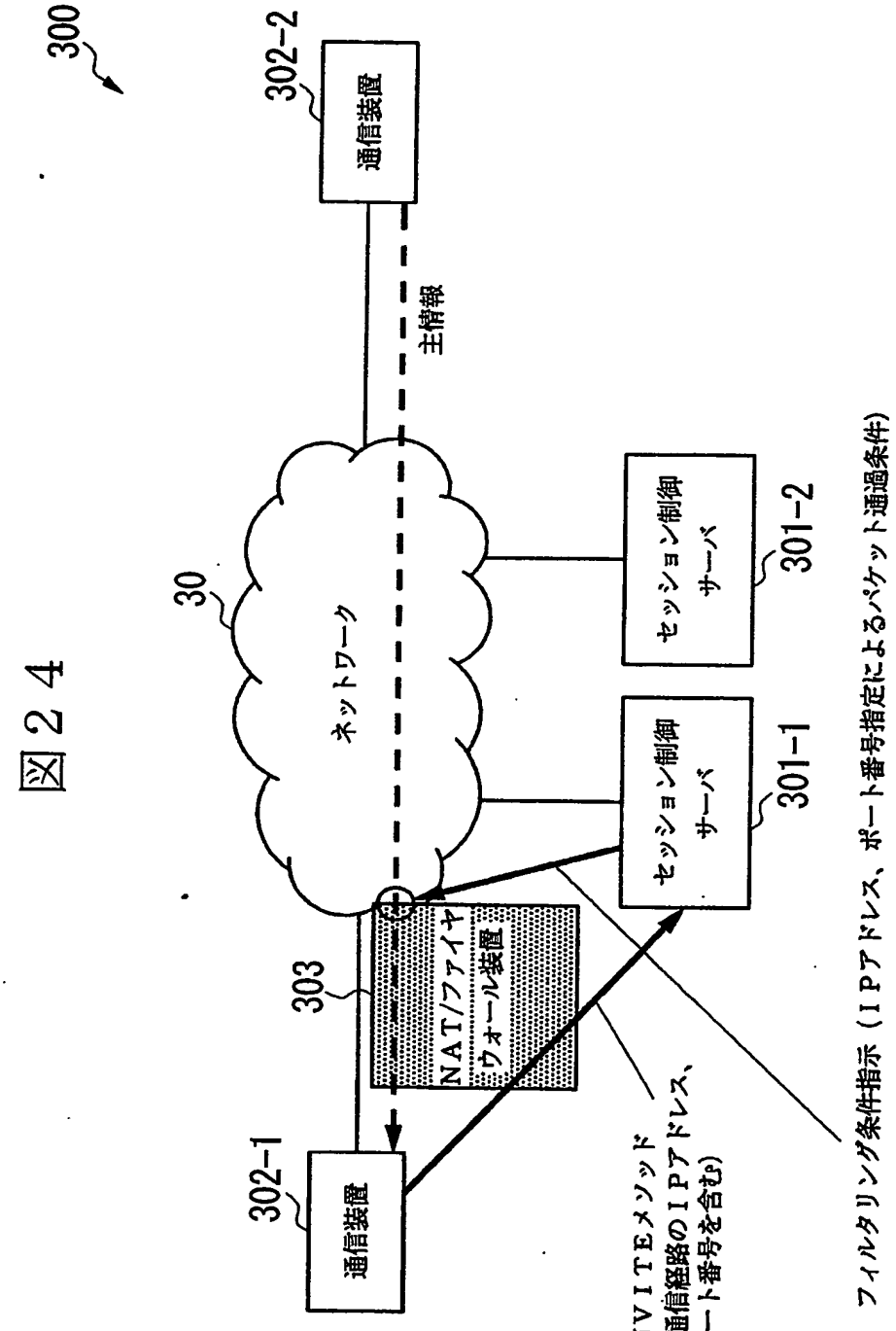
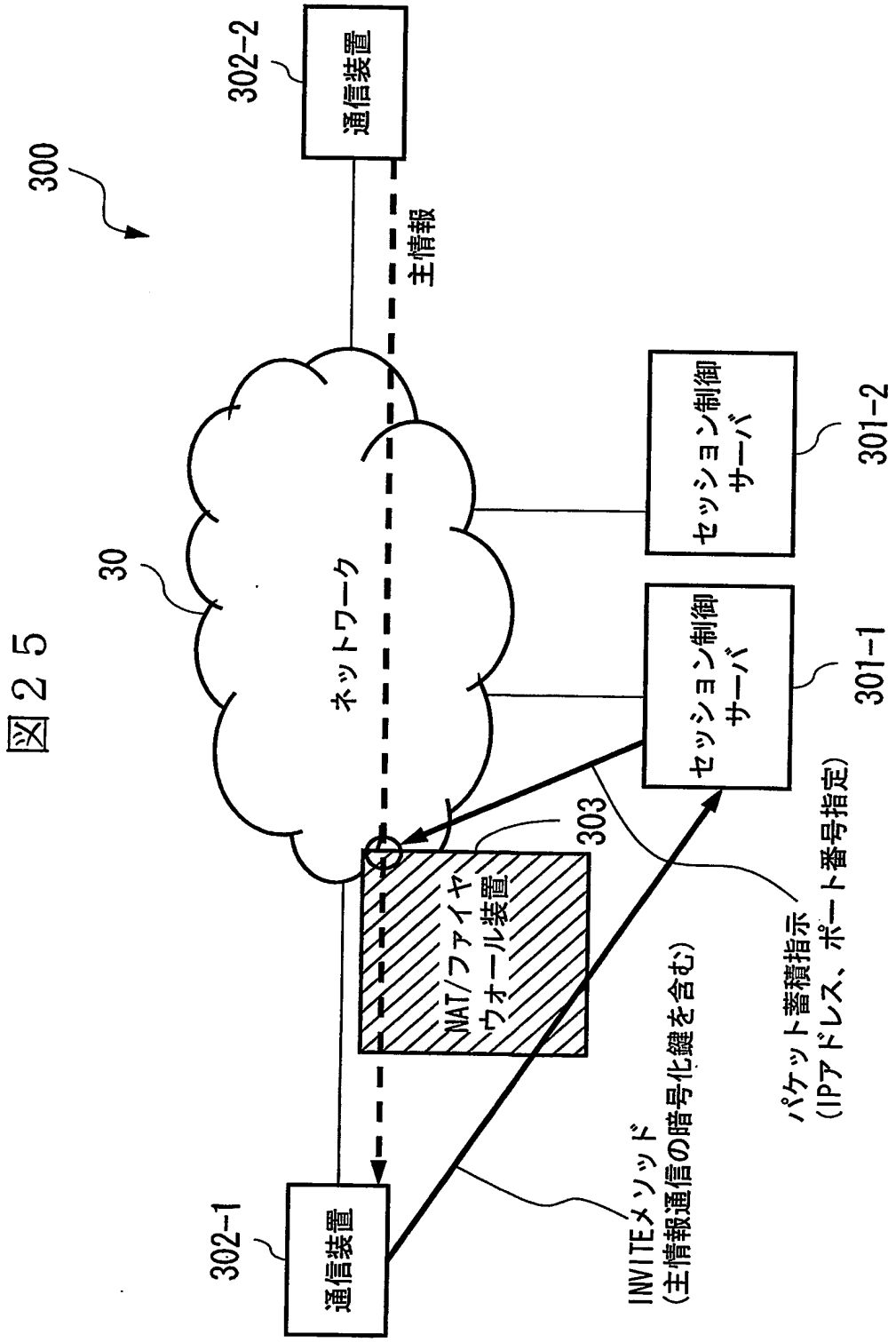

300
302-2
通信装置
主情報
30
ネットワーク
セッション制御
サーバ
301-2
セッション制御
サーバ
301-1
303
NAT/ファイヤ
ウォール装置
302-1
通信装置
INVITEメソッド
(主情報通信経路のIPアドレス、
ポート番号を含む)
フィルタリング条件指示（IPアドレス、ポート番号指定によるパケット通過条件）

図25


300
302-2
通信装置
主情報
30
ネットワーク
セッション制御
サーバ
301-2
セッション制御
サーバ
301-1
303
NAT/ファイヤ
ウォール装置
パケット蓄積指示
(IPアドレス、ポート番号指定)
INVITEメソッド
(主情報通信の暗号化鍵を含む)
302-1
通信装置

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/008942

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08, G06F13/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/08, G06F13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2003-108527 A (Microsoft Corp.), 11 April, 2003 (11.04.03), Full text; all drawings & EP 1267548 A2 & US 2003/005280 A1	1-10,12,14
X	JP 2000-250832 A (Oki Electric Industry Co., Ltd.), 14 September, 2000 (14.09.00), Full text; all drawings (Family: none)	11,13,15
X	JP 2000-59352 A (Murata Machinery Ltd.), 25 February, 2000 (25.02.00), Full text; all drawings (Family: none)	16-28,31,34, 37-50,53,56

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05 November, 2004 (05.11.04)	22 November, 2004 (22.11.04)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/008942

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2003-502757 A (ALCATEL INTERNETWORKING INC.), 21 January, 2003 (21.01.03), Full text; all drawings & WO 2000/78004 A2 & AU 200054868 A & EP 1143660 A & EP 1143661 A & EP 1143662 A & EP 1143663 A & EP 1143664 A & EP 1143665 A & EP 1143681 A & EP 1145519 A & US 6678835 B1 & US 6708187 B1 & CN 1483270 A	29,30,32,33, 35,36,51,52, 54,55,57,58

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/008942

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

(See extra sheet)

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

Continuation of Box No.III of continuation of first sheet(2)

The inventions of this application are divided into the following 27 groups of inventions:

1. claims 1, 2
2. claims 3, 4
3. claims 5, 6
4. claims 7-9
5. claim 10
5. claims 11, 13, 15
6. claims 12, 14
7. claims 16, 20, 22,
8. claims 17, 18, 23
9. claims 19, 21
10. claim 24
11. claim 25
12. claim 26
13. claim 27
14. claim 28
15. claims 29, 32, 35
16. claims 30. 33, 36
17. claims 31, 34
18. claims 37, 42, 43, 45
19. claims 38, 39, 40, 46
20. claims 41, 44
21. claims 47, 48, 49
22. claim 50
23. claim 51
24. claim 52
25. claims 53, 56
26. claims 54, 57, and
27. claims 55, 58.

国際調査報告

国際出願番号 PC[redacted]JP2004/008942

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl⁷ H04L 9/08, G06F13/00

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl⁷ H04L 9/08, G06F13/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2004年
日本国登録実用新案公報	1994－2004年
日本国実用新案登録公報	1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2003-108527 A (マイクロソフトコーポレイション) 2003.04.11, 全文全図を参照 & EP 1267548 A2 & US 2003/005280 A1	1-10, 12, 14
X	JP 2000-250832 A (沖電気工業株式会社) 2000.09.14, 全文全図を参照 (ファミリなし)	11, 13, 15
X	JP 2000-59352 A (村田機械株式会社) 2000.02.25, 全文全図を参照 (ファミリなし)	16-28, 31, 34, 37-50, 53, 56

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 05.11.2004	国際調査報告の発送日 22.11.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA/JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 中里 裕正　5M 9364 電話番号 03－3581－1101 内線 3599

様式PCT/ISA/210（第2ページ）（2004年1月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2003-502757 A (アルカテル・インターネットワーキング・インコーポレイテッド) 2003.01.21, 全文全図を参照　& WO 2000/78004 A2 & AU 200054868 A & EP 1143660 A & EP 1143661 A & EP 1143662 A & EP 1143663 A & EP 1143664 A & EP 1143665 A & EP 1143681 A & EP 1145519 A & US 6678835 B1 & US 6708187 B1 & CN 1483270 A	29, 30, 32, 33, 35, 36, 51, 52, 54, 55, 57, 58

国際調査報告

国際出願番号　PC[redacted]JP2004/008942

第Ⅱ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、

2．☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

別紙を参照。

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

この出願の発明は、以下の27群の発明に区分される。

1. 請求の範囲1, 2
2. 請求の範囲3, 4
3. 請求の範囲5, 6
4. 請求の範囲7-9
5. 請求の範囲10
5. 請求の範囲11, 13, 15
6. 請求の範囲12, 14
7. 請求の範囲16, 20, 22
8. 請求の範囲17, 18, 23
9. 請求の範囲19, 21
10. 請求の範囲24
11. 請求の範囲25
12. 請求の範囲26
13. 請求の範囲27
14. 請求の範囲28
15. 請求の範囲29, 32, 35
16. 請求の範囲30, 33, 36
17. 請求の範囲31, 34
18. 請求の範囲37, 42, 43, 45
19. 請求の範囲38, 39, 40, 46
20. 請求の範囲41, 44
21. 請求の範囲47, 48, 49
22. 請求の範囲50
23. 請求の範囲51
24. 請求の範囲52
25. 請求の範囲53, 56
26. 請求の範囲54, 57
27. 請求の範囲55, 58

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.